RouteFinder™
Internet Security Appliance

RF550VPN and RF560VPN

RF550VPN/RF560VPN Using a NAT Box with IPSec Pass-Through

Reference Guide

MultiTech® Systems

How-To: RF550VPN/RF560VPN Using a NAT Box with IPSec Pass-Through

Copyright © 2003
This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved. Multi-Tech Systems, Inc. makes no representations or warranty with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Reference Guide Number: S000259C

Revision	Date	Description
A	06/07/02	Initial release.
B	04/17/03	Changes for software Version 4.64.
C	07/07/03	Add RF560VPN.

The examples on the following pages illustrate:

1. SSH Sentinel IPSec client behind a NAT box doing IPSec Pass-Through to a RF550VPN/RF560VPN.

2. RF550VPN/RF560VPN, behind a NAT box, doing IPSec Pass-Through to another RF550VPN/RF560VPN.

The RouteFinder software is pre-installed on the RF550VPN/RF560VPN RouteFinder. **RF550VPN/RF560VPN firmware version 4.62 or higher is required to support IPSec Pass-Through.** Initial configuration is required in order for you to run the RouteFinder software and begin operation. The browser-based interface eases VPN configuration and management. The VPN functionality is based on IPSec and PPTP protocols and uses 168-bit Triple DES encryption to ensure that your information remains private.

Caution: **Use a safe Password!** Your first name spelled backwards is not a sufficiently safe password; a password such as **xfT35$4** is better.

Example 1

This example provides a sample RouteFinder configuration and related address scheme for an application employing Client-to-LAN IPSec Pass-Through communication. This is an example on how to configure an RF550VPN/RF560VPN at Site A and an SSH Sentinel client behind a NAT box at Site B, so that Site A and B can communicate through a secure connection over the Internet using IPSec Pass-Through. This example shows Site B using a static or dynamic IP address.

The diagram shows a RouteFinder 550VPN, but it can also be a RouteFinder 560VPN.

SSH IPSec Client behind a NAT doing IPSec pass through to a RouteFinder 550/560VPN

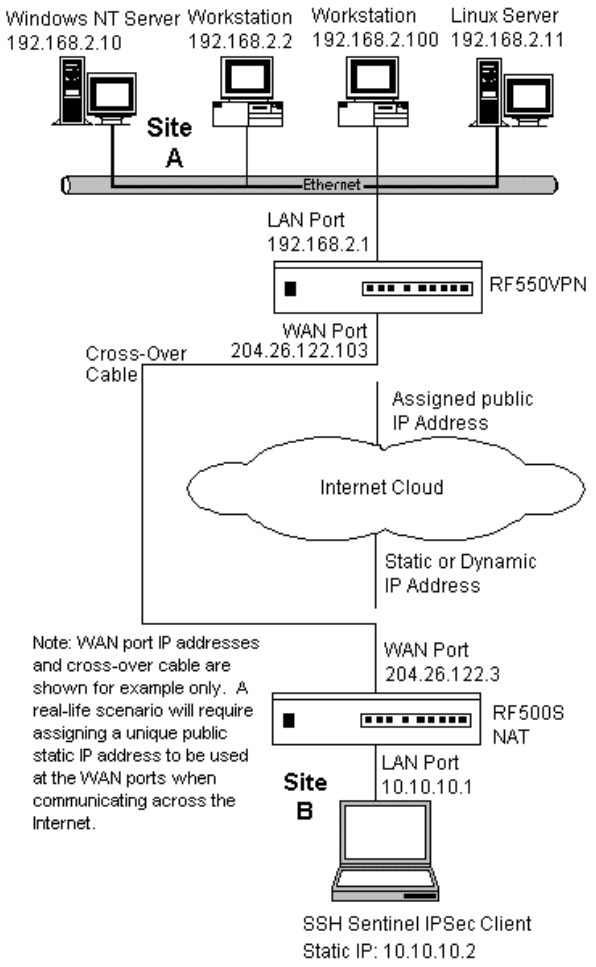
1. Domain name = Site-A.com

2. Public Class C = 204.26.122.x

3. SETUP WIZARD > DEVICE IP SETTINGS
   IP Address: 192.168.2.1
   IP Subnet Mask: 255.255.255.0

4. SETUP WIZARD > ISP SETTINGS
   Select 'Static IP Settings'
   IP assigned by your ISP: 204.26.122.103
   IP Subnet Mask: 255.255.255.0
   ISP Gateway Address: 204.26.122.3

5. SETUP WIZARD > VPN SETTINGS
   Connection Name = IPSec Pass-Through
   Enable 'Enable UID" (Unique Identifier String)
   Local IPSEC Identifier = 204.26.122.103
   Remote IPSEC Identifier = 192.168.10.0
   Disable (do not check) 'Enabled Keep Alive'
   Disable (do not check) 'Enabled NetBIOS Broadcast'
   Remote Site = LAN
   Remote IP Network = 10.10.10.2
   Remote IP Netmask = 255.255.255.0
   Remote Gateway IP/FQDN = 204.26.122.3 (static)
   Remote Gateway IP/FQDN = 0.0.0.0 (dynamic)
   Network Interface = WAN ETHERNET
   Secure Association = check IKE
   Perfect Forward Secure = check enabled
   Encryption Protocol = select 3DES
   Preshared Key = (must match key code at Site B)
   Key Life = set to default
   IKE Life Time = set to default


Windows NT Server 192.168.2.10
Workstation 192.168.2.2
Workstation 192.168.2.100
Linux Server 192.168.2.11
Site A
Ethernet
LAN Port 192.168.2.1
RF550VPN
WAN Port 204.26.122.103
Cross-Over Cable
Assigned public IP Address
Internet Cloud
Static or Dynamic IP Address
Note: WAN port IP addresses and cross-over cable are shown for example only. A real-life scenario will require assigning a unique public static IP address to be used at the WAN ports when communicating across the Internet.
WAN Port 204.26.122.3
RF500S NAT
LAN Port 10.10.10.1
Site B
SSH Sentinel IPSec Client
Static IP: 10.10.10.2

Note: Make sure that all routers between both SSH IPSec ends can route IP protocol 50 (IPSec). Sometimes routers are configured to route only TCP (protocol 6), UDP (protocol 17) and ICMP (Protocol 1) and drop all other protocols. VPN routers configured that way won't work with IPSec!

Software Configuration

Example 1: Configuration Procedure at Site A

1. Connect a workstation to one of the RF550VPN/RF560VPN's **LAN ports** via Ethernet at Site A.

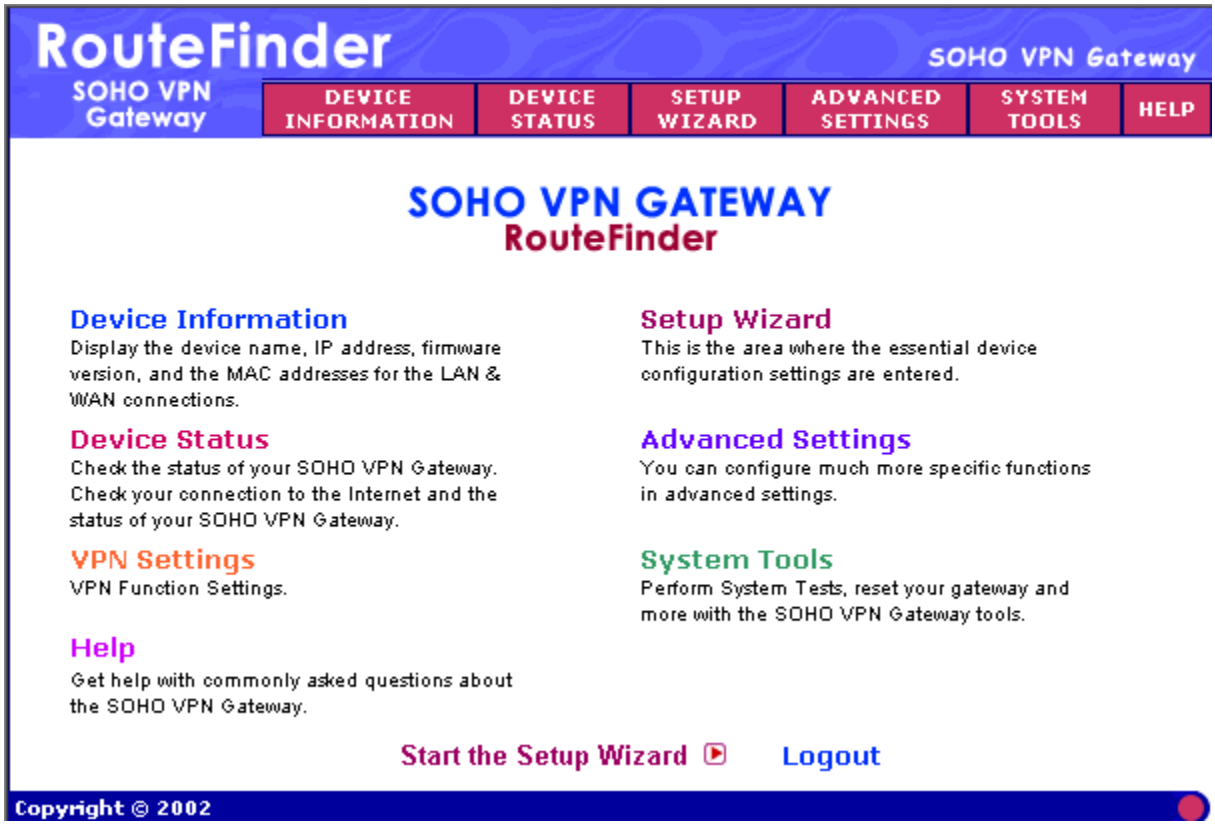
2. Set the workstation IP address to 192.168.2.x subnet.

3. Apply power to the RF550VPN/RF560VPN RouteFinder and allow the LEDs to stabilize on the unit.

4. Bring up your web browser on the workstation. At the web browser's address line, type the Gateway address of http://192.168.2.1 and hit the **Enter** key.

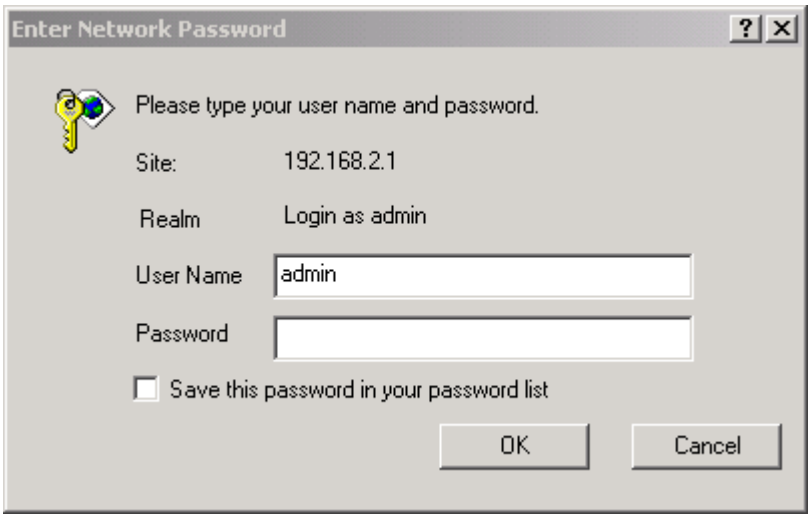
Note: Make sure your workstation's IP address is in the same network as the router's address. **WINIPCFG** and **IPCONFIG** are tools for finding a computer's default gateway and MAC address. In Windows 98/Me you can type **WINIPCFG**. In Windows 2000/NT, you can type **IPCONFIG**.

5. After typing the IP Address in the web browser, the RF550VPN/RF560VPN main menu displays.


RouteFinder
SOHO VPN Gateway
SOHO VPN Gateway
DEVICE INFORMATION
DEVICE STATUS
SETUP WIZARD
ADVANCED SETTINGS
SYSTEM TOOLS
HELP
SOHO VPN GATEWAY
RouteFinder
Device Information
Display the device name, IP address, firmware version, and the MAC addresses for the LAN & WAN connections.
Device Status
Check the status of your SOHO VPN Gateway. Check your connection to the Internet and the status of your SOHO VPN Gateway.
VPN Settings
VPN Function Settings.
Help
Get help with commonly asked questions about the SOHO VPN Gateway.
Setup Wizard
This is the area where the essential device configuration settings are entered.
Advanced Settings
You can configure much more specific functions in advanced settings.
System Tools
Perform System Tests, reset your gateway and more with the SOHO VPN Gateway tools.
Start the Setup Wizard
Logout
Copyright © 2002

6. On the Main Menu, click the **Setup Wizard** button. The **Password** dialog box displays.

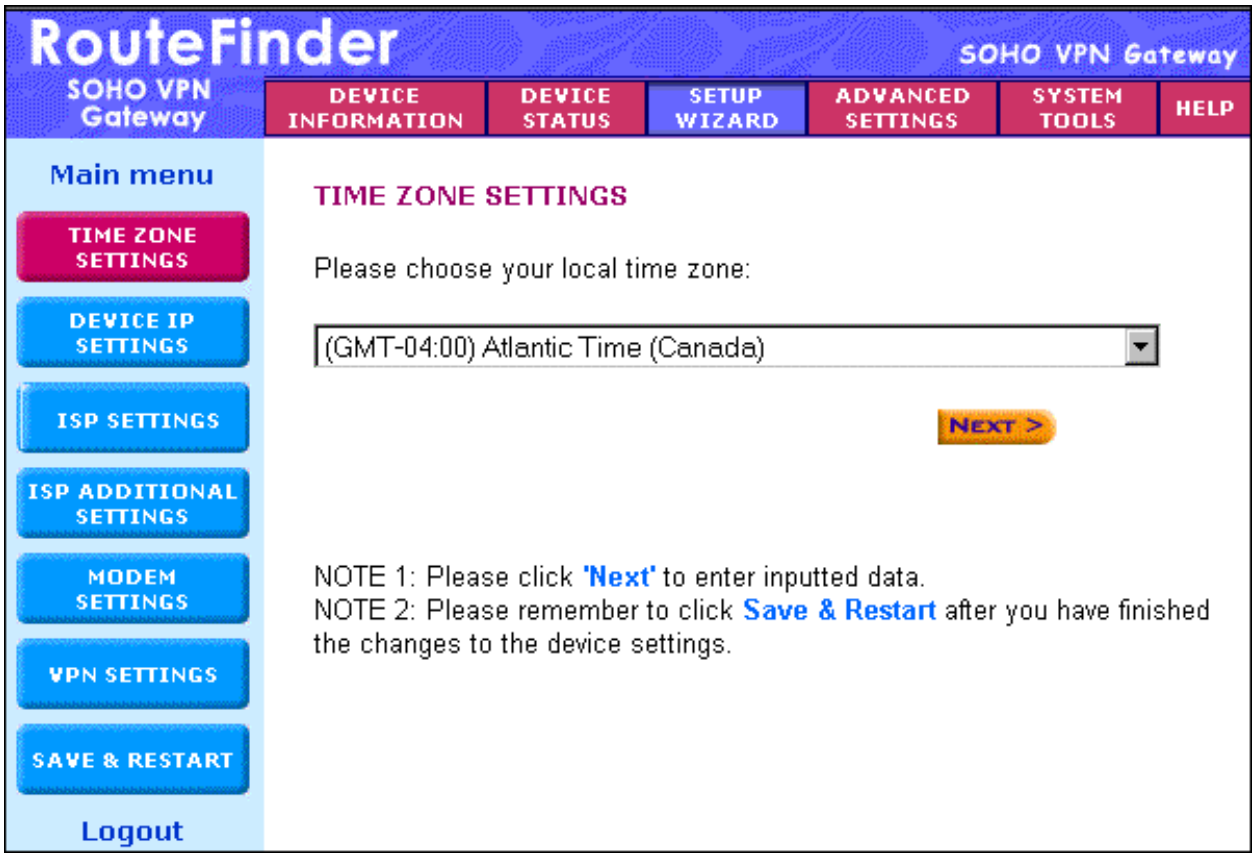
7. Type **admin** (**admin** is the default user name) in the user name box and leave the password box empty.



Note: To change your password after logging in, select the **Advanced Settings** button and **Administrative Settings**.

8. Click **OK**. The **Setup Wizard** screen displays a step-by-step process that lets you input all of the basic settings to configure your RF550VPN/RF560VPN.

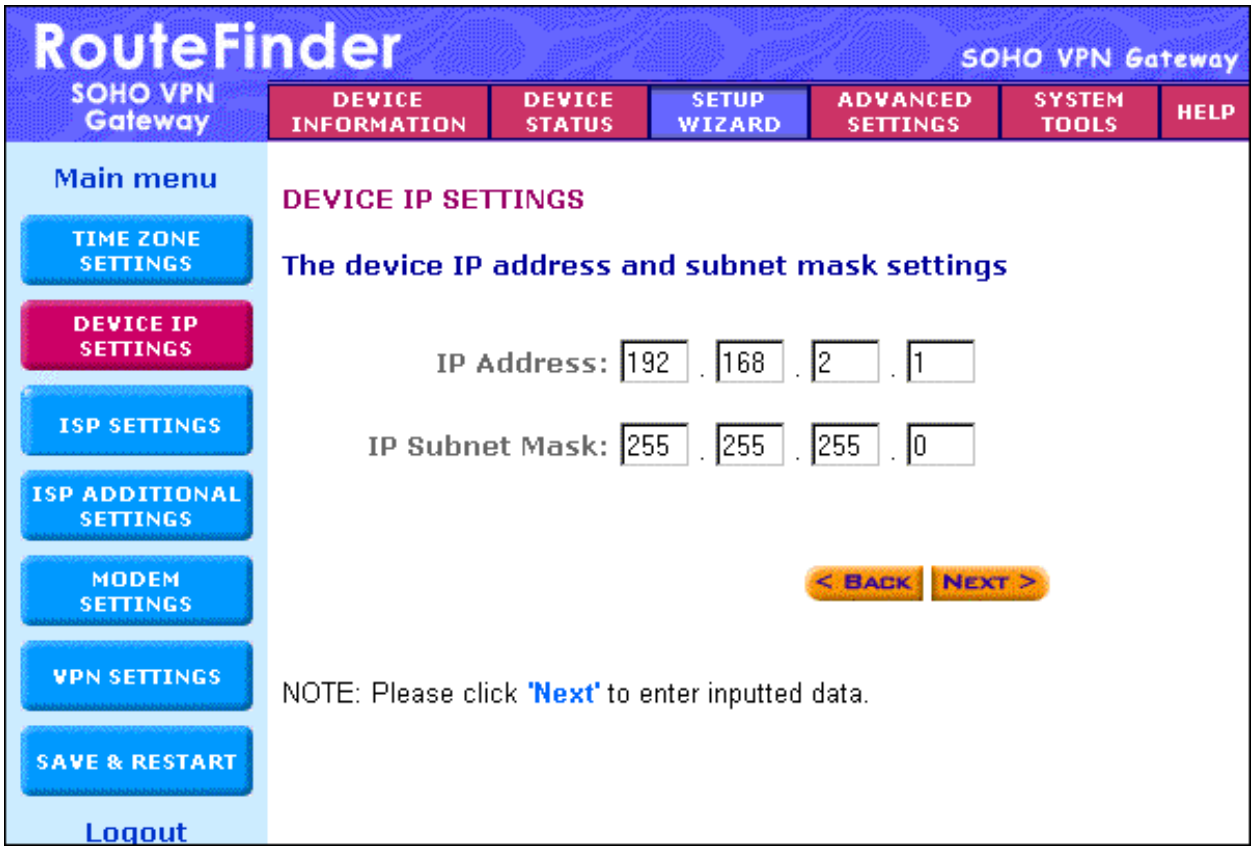
9. Select the **Time Zone**, and then click the **Next** button to continue.



10. For **Device IP Settings** enter the internal LAN IP address and subnet mask that you want assigned to the LAN ports of the RF550VPN/RF560VPN. This is not the IP address from your ISP but the local internal LAN IP address. The default IP address is **192.168.2.1** and will be used for our example.

    Device IP Address: 192.168.2.1.
    Device IP Subnet Mask: 255.255.255.0

    Click the **Next** button.



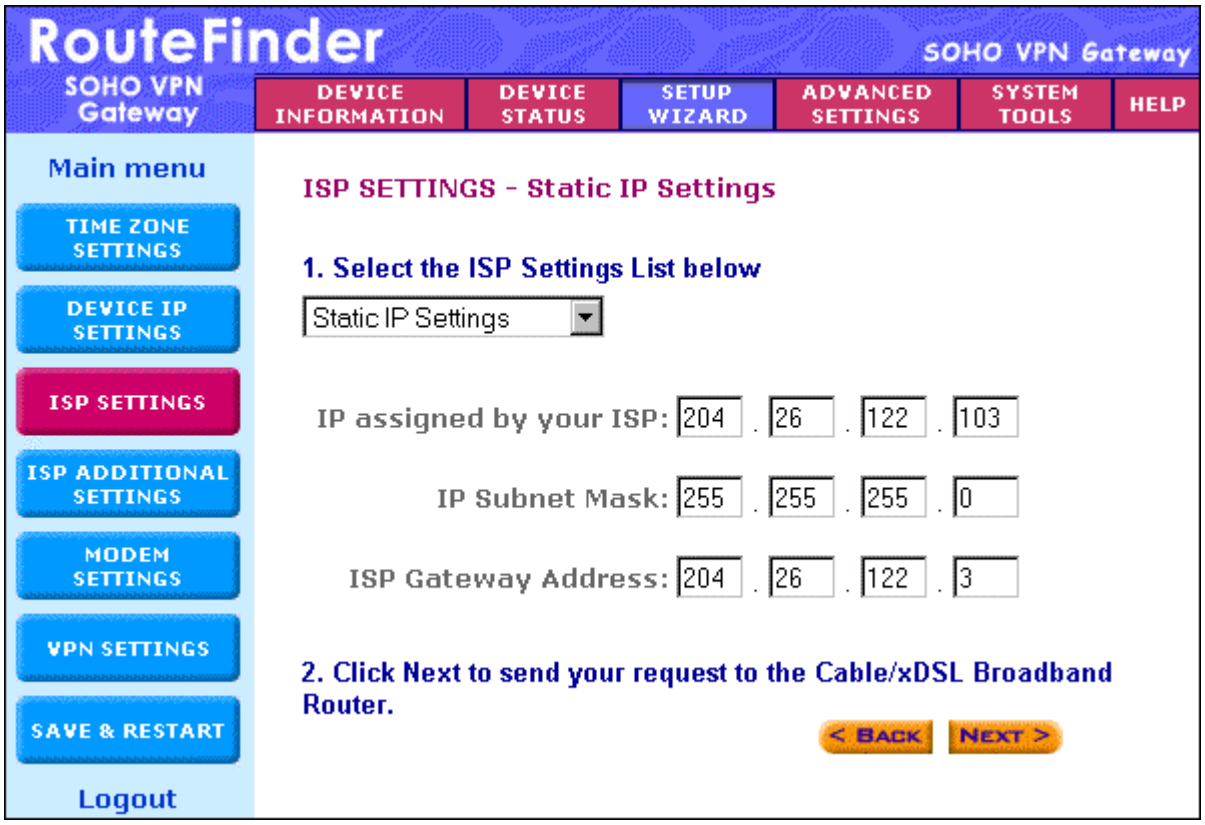
11. On the ISP Settings screen, select **Static IP Settings** and enter the following information.

    a) **IP Assigned by your ISP:** This is the IP address of the WAN port on the RF550VPN/RF560VPN at Site A.
    (Ex: 204.26.122.103)

    b) **IP Subnet Mask:** This is the IP address of the subnet mask for the WAN port on the RF550VPN/RF560VPN.
    (Ex: 255.255.255.0)

    c) **IP Gateway Address:** This is the IP address of the WAN port on the RF550VPN/RF560VPN at Site B.
    (Ex: 204.26.122.3)

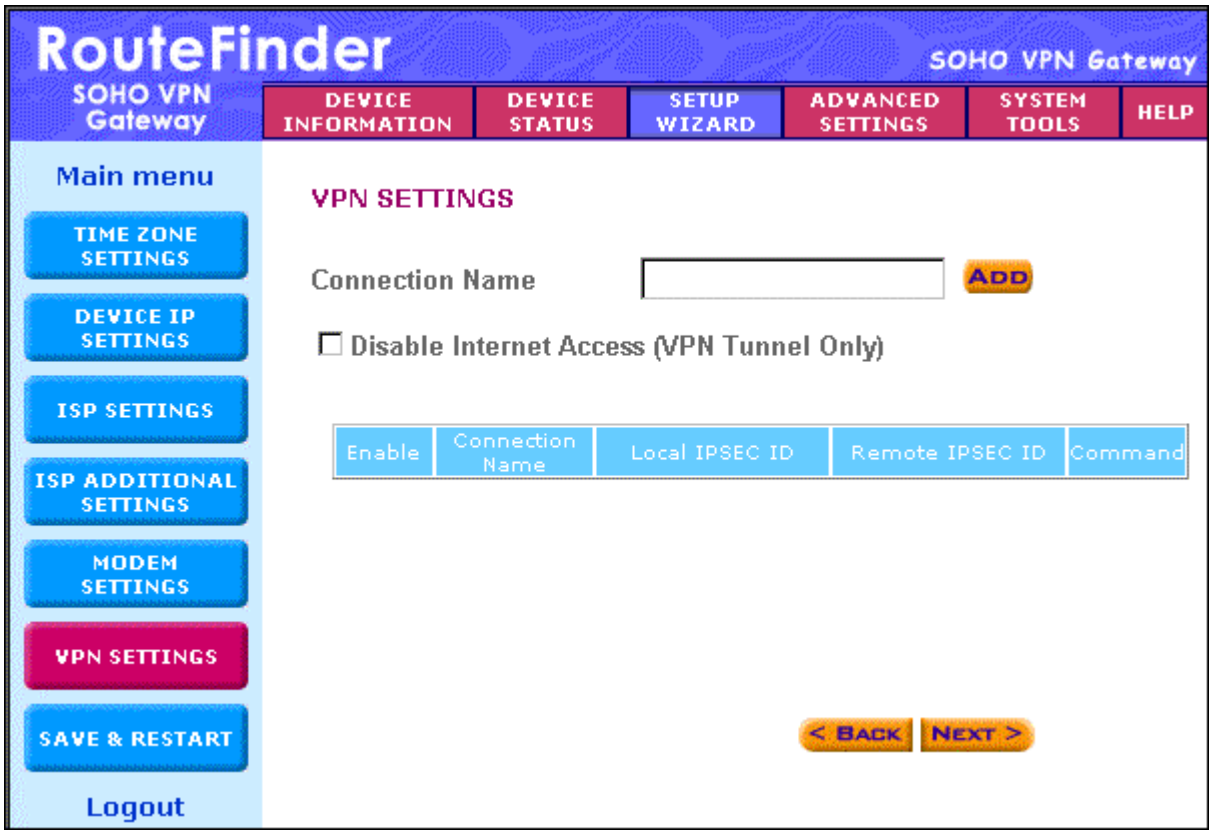
    Click the **Next** button.


RouteFinder
SOHO VPN Gateway
SOHO VPN Gateway
DEVICE INFORMATION
DEVICE STATUS
SETUP WIZARD
ADVANCED SETTINGS
SYSTEM TOOLS
HELP
Main menu
TIME ZONE SETTINGS
DEVICE IP SETTINGS
ISP SETTINGS
ISP ADDITIONAL SETTINGS
MODEM SETTINGS
VPN SETTINGS
SAVE & RESTART
Logout
ISP SETTINGS - Static IP Settings
1. Select the ISP Settings List below
Static IP Settings
IP assigned by your ISP: 204 . 26 . 122 . 103
IP Subnet Mask: 255 . 255 . 255 . 0
ISP Gateway Address: 204 . 26 . 122 . 3
2. Click Next to send your request to the Cable/xDSL Broadband Router.
< BACK
NEXT >

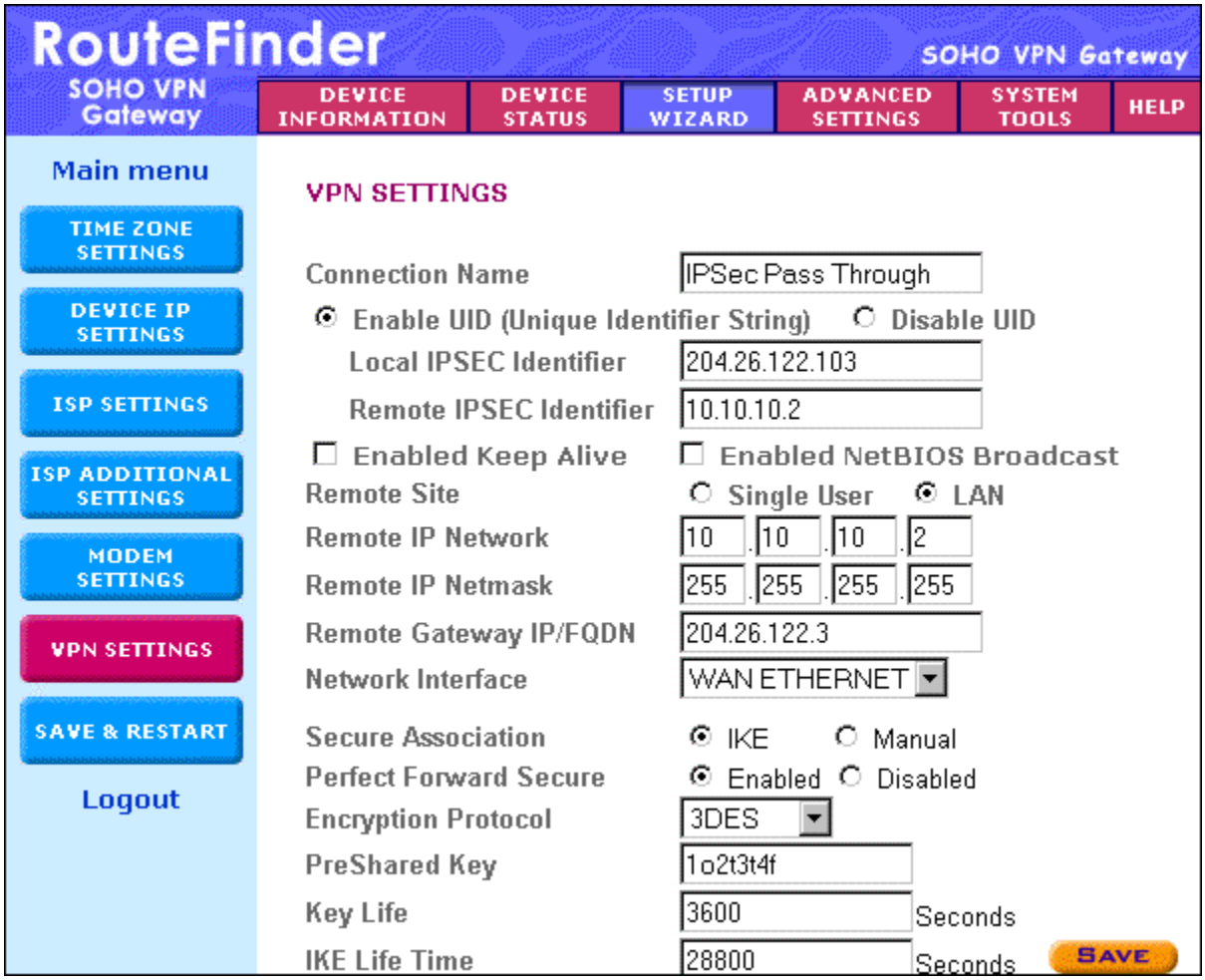
Note: For this scenario of connecting two RouteFinders back-to-back it is not necessary to enter any information for the **ISP Additional Settings** or **Modem Settings**.

12. Click the button on the left side of the screen for **VPN Settings**. Use this screen to setup your LAN-to-LAN VPN connection.

13. **For the RF550VPN:** In the **Connection Name** field, type a name that identifies for you a connection that you would like to make. (Ex: **IPSec Pass Through**). Click the **Add** button.



14. The **VPN Settings** screen for entering specific VPN settings will display. The screen pictured below assumes **IKE** is selected as the **Secure Association**. The **Connection Name** (**IPSec Pass Through**) defaults into the first field. This screen can be configured to support the NAT box at Site B using a static or dynamic IP address. Continue to enter the following settings:



a) Select **Enable UID (Unique Identifier String)**

b) **Local IPSec Identifier:** Enter the IP address that identifies the Local IPSec for this connection. Example: 204.26.122.103

c) **Remote IPSec Identifier:** Enter the IP address that identifies the Remote IPSec for this connection. Example: 10.10.10.2

d) Disable (do not check) **Enabled Keep Alive**

e) Disable (do not check) **Enabled NetBIOS Broadcast**

f) **Remote Site:** LAN

g) **Remote IP Network:** Enter the remote IP address (SSH client) for Site B. Example: 10.10.10.2

h) **Remote IP Netmask:** Enter the remote IP Netmask (SSH client) for Site B. Example: 255.255.255.255

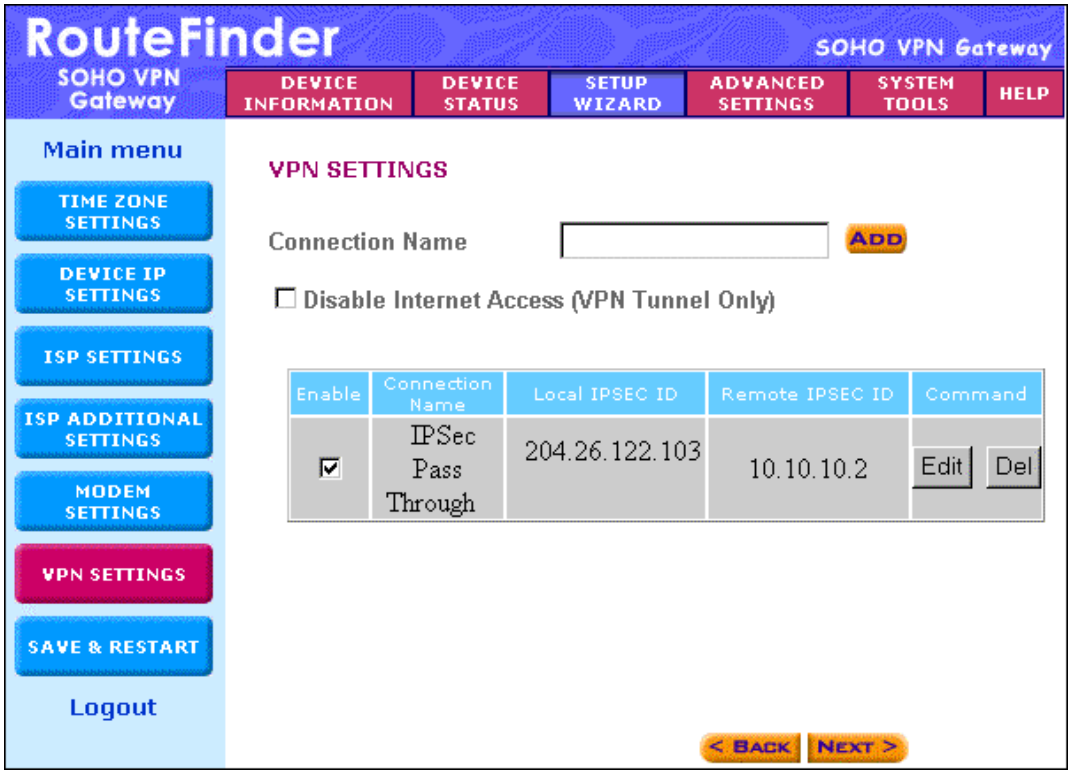
i) **Remote Gateway IP/FQDN:** Enter the Remote Gateway IP address (WAN) for Site B. Example: 204.26.122.3 for static or 0.0.0.0 for dynamic)

j) **Network Interface:** Select the Network Interface from the drop-down list box.
Example: WAN ETHERNET

k) **Secure Association:** Select **IKE** (the default) to set how inbound packets will be filtered. IKE primarily encompasses router key exchange and the negotiation of security policy. Selecting IKE will cause the following fields to display.

- **Perfect Forward Secure:** Check **Enabled**
- **Encryption Protocol:** Select the encryption protocol used for your configuration. The default protocol for the RF550VPN/RF560VPN communicating with another RF550VPN/RF560VPN is **3DES**.
- **Preshared Key:** Enter the PreShared Key name. You can enter an alphanumeric name, (Ex. 1o2t3t4f), but it must match the security code for the RouteFinder at Site B.
- **Key Life:** Enter the amount of time that tells the router to renegotiate the Key. For example 3600 seconds is 60 minutes
- **IKE Life Time:** Enter the amount of time that tells the router to renegotiate the IKE security association. For example 28800 seconds is 8 hours.

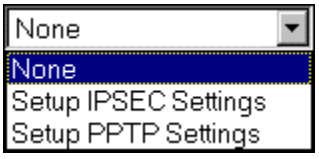
15. Once the VPN settings are entered, click the **Save** button. The data will be displayed on the VPN Settings screen where you can enable/disable, edit, or delete this connection:



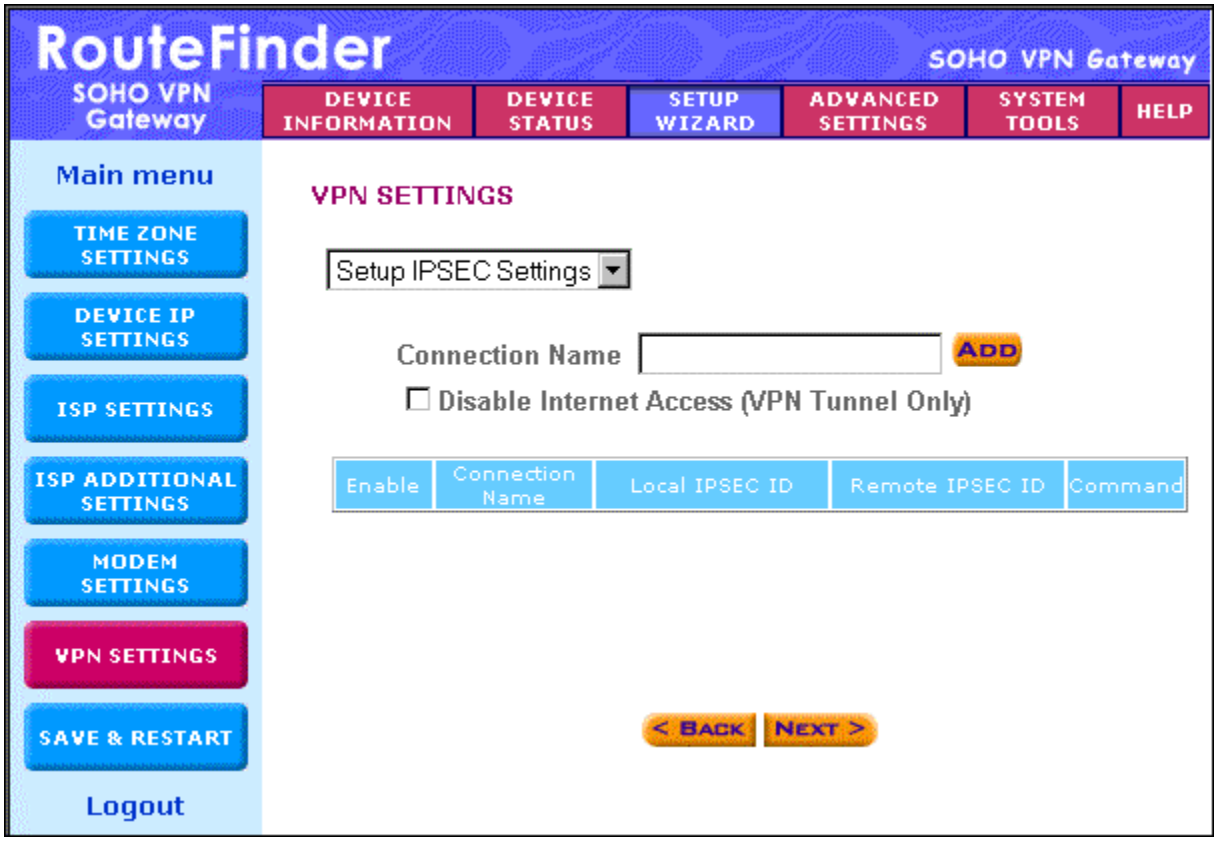
Note: If you uncheck the **Enable** box on this screen, the information will remain for you to enable/disable, edit, or delete at any time you desire.

For the RF560VPN:

From the **VPN Settings** drop-down list box, select the type of VPN Connection you want to set:



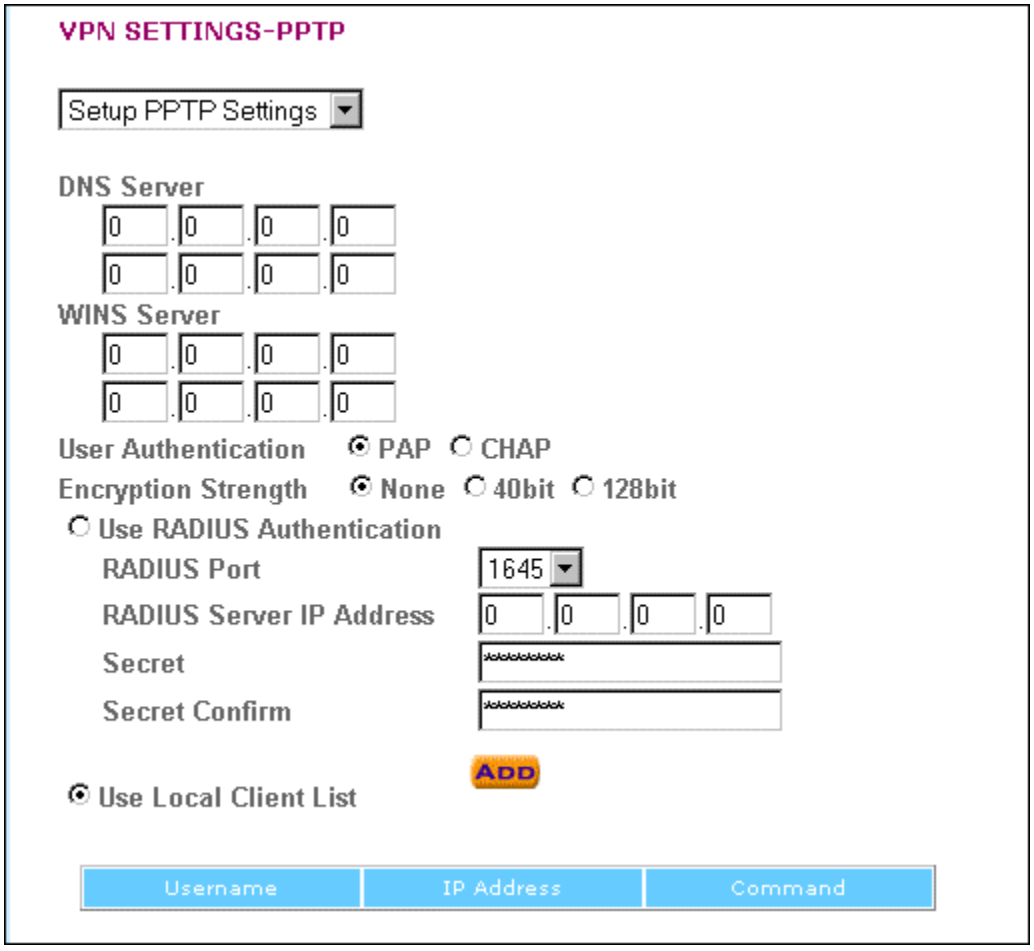
If you select Setup IPSEC Settings, the following screen displays:



- In the **Connection Name** field, type a name that describes a connection you would like to make.
- Example: **Site A**.
- Click the **Add** button, and the **VPN Settings** detail screen will display (see the next screen). Once you have entered the settings, the **Connection Name** displays on the lower half of the screen (above).
- Click the checkbox if you want to **Disable Internet Access (VPN Tunnel Only).**
- You can then edit, delete, or enable/disable this connection by clicking the corresponding buttons.
- To enable this connection, check the **Enable** box.

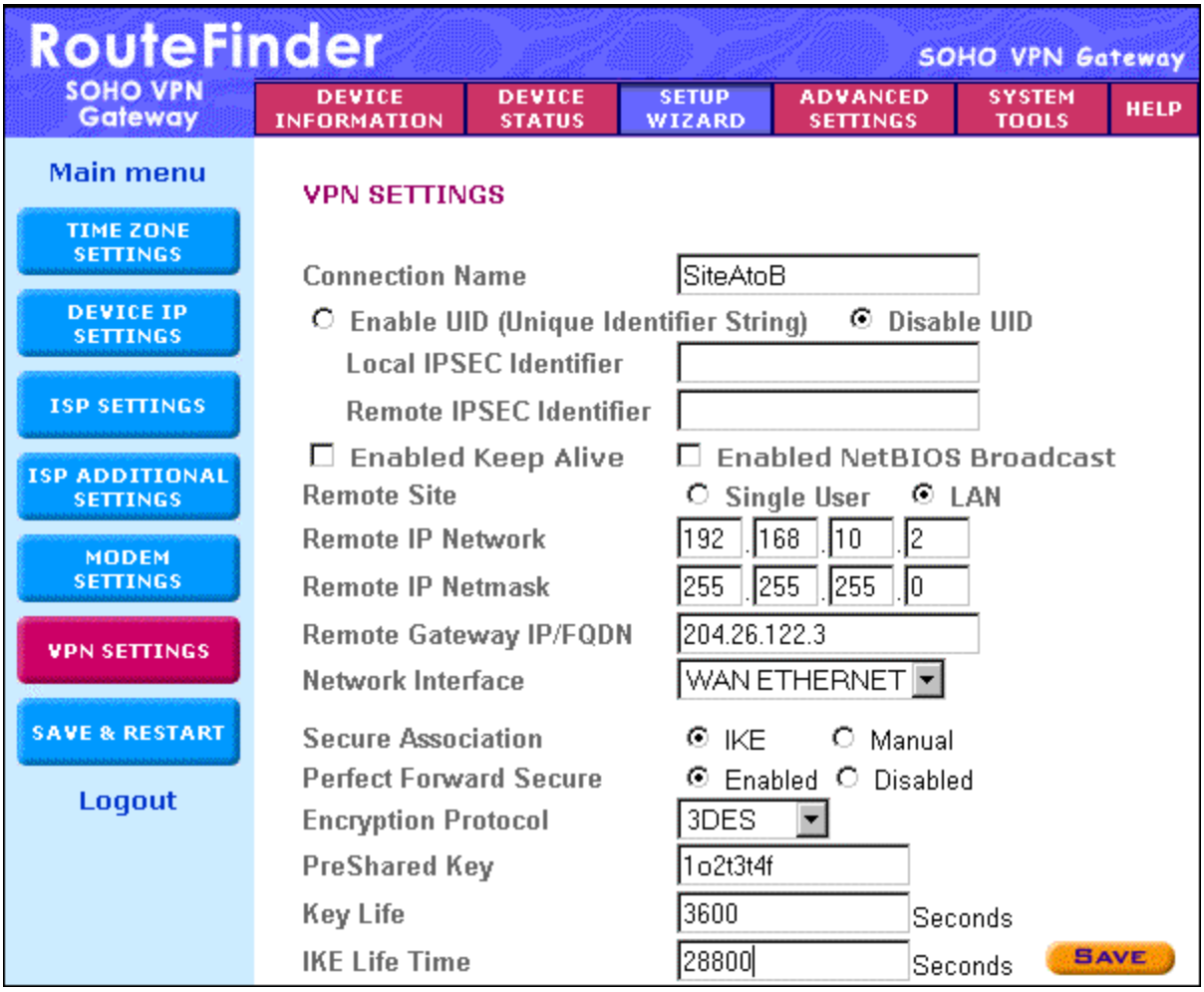
Note: If you uncheck the **Enable** box, the connection will not be active, but the parameters will remain on the screen for you to enable, edit, or delete as desired.

If you select Setup PPTP Settings, the following screen displays:



- **DNS Server** – Enter the address of the DNS Server to be used.
- **WINS Server** – Enter the address of WINS Server to be used.
- **User Authentication** – Select the User Authentication method to be used.
- **Encryption Strength** – Select the Encryption Strength desired.
- **Use RADIUS Authentication:**
  Check the Use RADIUS Authentication button to enable RADIUS. Then the following information:
  - **RADIUS Port** – Select the port number.
  - **RADIUS Server IP Address** – Enter the RADIUS Server IP Address.
  - **Secret** – Enter a secret password.
  - **Secret Confirm** – Retype the secret password for verification.
- **Use Local Client List** – Check this radio button to have your local client list used by the program.

14a. The **VPN Settings** screen for entering specific VPN settings will display. The screen pictured below assumes **IKE** is selected as the **Secure Association**. The **Connection Name** (**SiteAtoB**) defaults into the first field. Two configuration choices are available for the Secure Association: **IKE** and **Manual**.



a) Select **Disable UID** and leave **Local IPSec Identifier** and **Remote IPSec Identifier** blank.

b) Do **not** check **Enabled Keep Alive**.

c) Do **not** check **Enabled NetBIOS Broadcast**.

d) **Remote Site –** Select **LAN.**

e) **Remote IP Network –** Enter the **Remote IP Network** address (**LAN**) for Site B.

f) (Ex: **192.168.10.0**)

g) **Remote IP Netmask –** Enter the **Remote IP Netmask** address for Site B. (Ex: **255.255.255.0**)

h) **Remote Gateway IP –** Enter the **Remote Gateway IP** address (**WAN**) for Site B.

i) (Ex: **204.26.122.3**)

j) **Network Interface –** Select the **Network Interface** from the drop-down list box. (Ex: **WAN Ethernet**)

k) **Secure Association –** Select **IKE** to set how inbound packets will be filtered. **IKE** is the default. **IKE** primarily encompasses router key exchange and the negotiation of security policy. Selecting **IKE** will display the following fields.

l) **Perfect Forward Secure –** Check the **Enabled** button.

m) **Encryption Protocol** – Select the encryption protocol used for your configuration. The default protocol for the RF550VPN/RF560VPN communicating with another RF550VPN/RF560VPN is **3DES**. (Ex: **3DES**)

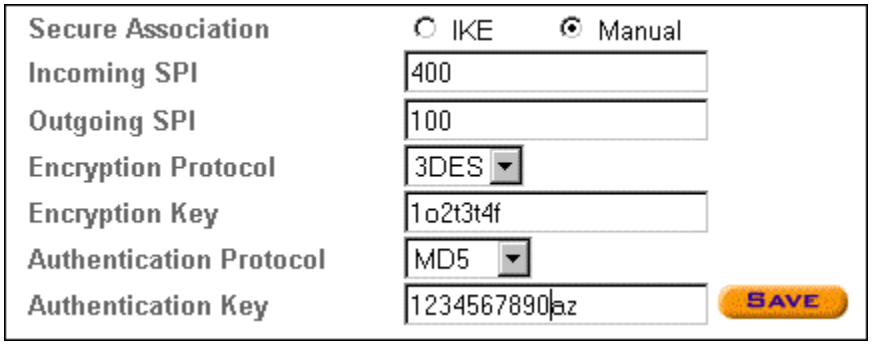
n) **PreShared Key –** Enter the **PreShared Key** name (you can enter an alphanumeric name but it needs to match the security code for the RouteFinder at Site B).

o) **Key Life –** Enter the amount of time that tells the router to renegotiate the Key. For example, 3600 seconds is 60 minutes.

p) **IKE Life Time –** Enter the amount of time that tells the router to renegotiate the IKE security association. For example, 28800 seconds is 8 hours.

14b. The screen pictured below assumes **Manual** as the **Secure Association** is selected on the VPN Settings screen. The **Connection Name** (**SiteAtoB**) defaults into the first field. Continue to enter the following settings:

Note: If **Secure Association** is set to **Manual**, the two RF550VPN/RF560VPNs must communicate with Static IP addresses at both ends.



Note: Enter all data for **a)** through **h)** as illustrated above. Then complete the following:

i) **Secure Association –** Selecting **Manual** instead of **IKE** will set how inbound packets will be filtered and then the following fields display.

j) **Incoming SPI –** Enter the incoming SPI that the remote VPN gateway, at Site B, will use to identify this Security Association. Enter a three-digit number between 100 and 400. This value must match the outgoing SPI value entered at the remote VPN gateway at Site B. (Ex: 400)

k) **Outgoing SPI** – Enter the outgoing SPI that the Site A VPN gateway will use to identify this Security Association. Enter a three-digit number between 100 and 400. This value must match the incoming SPI value entered at the remote VPN gateway at Site B. (Ex: 100)

l) **Encryption Protocol** – Select an appropriate encryption algorithm: Null**, DES, 3DES**. **3DES** is the recommended choice.

m) **Encryption Key –** Enter a string of characters to be used to encrypt and decrypt transmitted data between the two RouteFinders. The string is made up of 8-16 alphanumeric characters and needs to match the **Encryption Key** for the RouteFinder at Site B. (Ex: 1o2t3t4f)

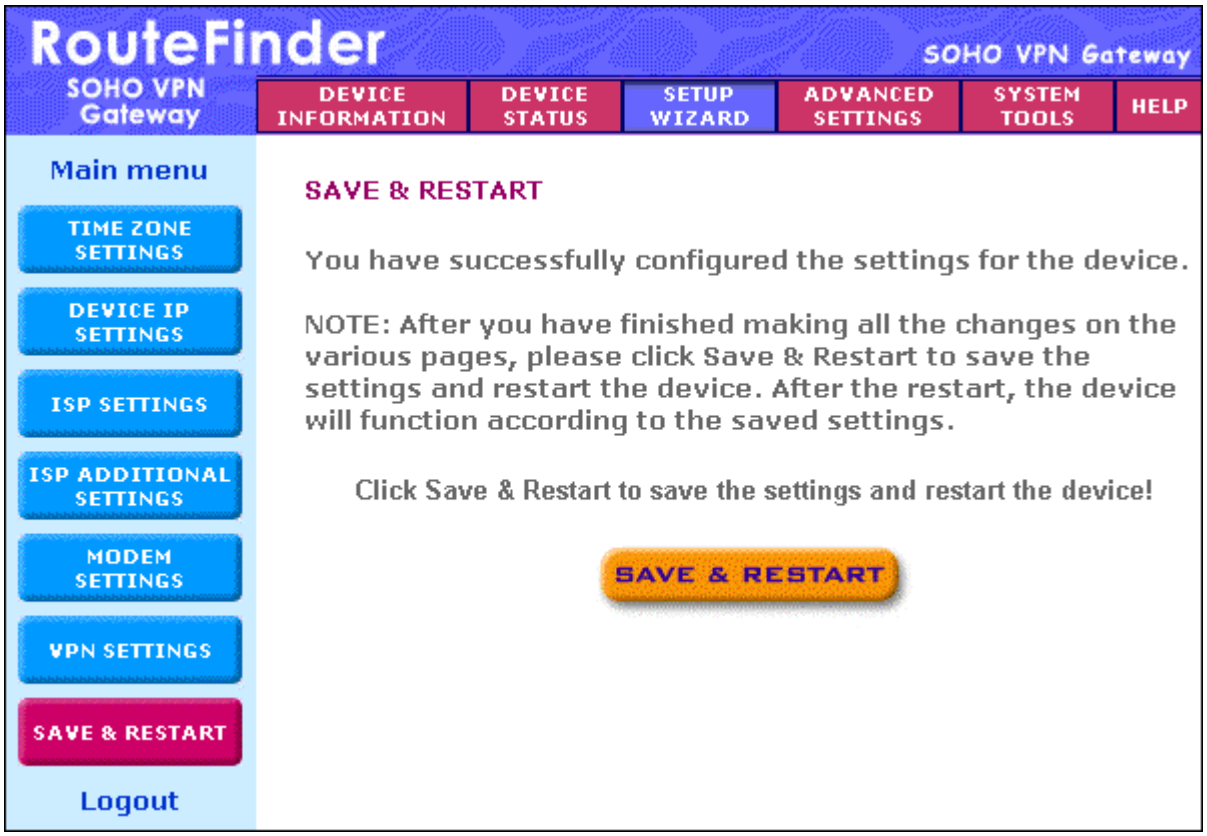
n) **Authentication Protocol** – Select an appropriate authentication algorithm: **MD5** or **SHA-1. MD5** is the recommended choice.

o) **Authentication Key –** Enter a string of characters to be used as a key for authentication between the two RouteFinders. The string is similar to a password and is made up of 8-16 alphanumeric characters and needs to match the **Authentication Key** for the VPN at Site B. (Ex: 1234567890az)

15. Once the VPN settings are entered, click on the **Save** button. The **Connection Name** will display on the lower half of the screen and on the initial VPN Settings screen. You can enable/disable, edit, or delete this connection by clicking the corresponding buttons. To enable this connection, check the **Enable** box that appears to the left of the connection name.

    Note: If you uncheck the **Enable** box, the parameters will remain in the table for you to enable/disable, edit, or delete at any time.

16. After you have finished entering the data and making any changes on the various screens, click the **Save and Restart** button to save the settings and restart the device**.** After the device restarts, it will function according to the saved settings.


RouteFinder
SOHO VPN Gateway
SOHO VPN Gateway
DEVICE INFORMATION
DEVICE STATUS
SETUP WIZARD
ADVANCED SETTINGS
SYSTEM TOOLS
HELP
Main menu
TIME ZONE SETTINGS
DEVICE IP SETTINGS
ISP SETTINGS
ISP ADDITIONAL SETTINGS
MODEM SETTINGS
VPN SETTINGS
SAVE & RESTART
Logout
SAVE & RESTART
You have successfully configured the settings for the device.
NOTE: After you have finished making all the changes on the various pages, please click Save & Restart to save the settings and restart the device. After the restart, the device will function according to the saved settings.
Click Save & Restart to save the settings and restart the device!
SAVE & RESTART

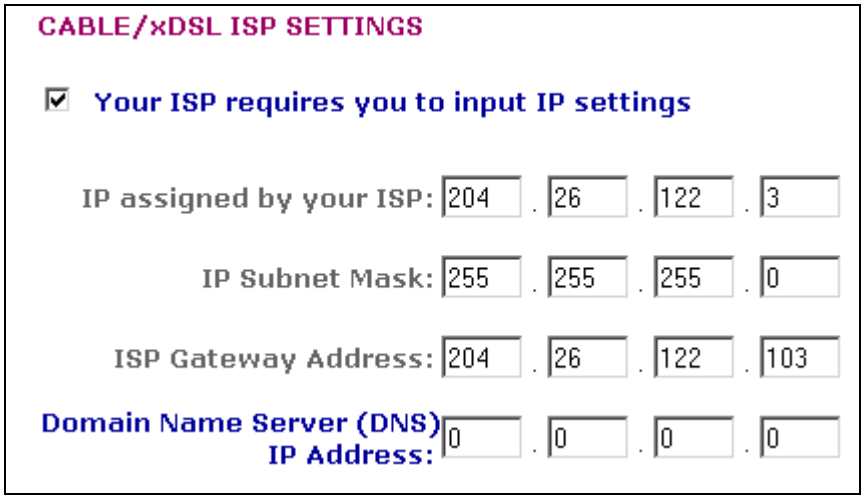
17. During the save and restart process, system messages will let you know that you have successfully configured the settings for the device and saved the settings. You will see a status bar across the bottom of your browser showing the progress of the startup process. The RouteFinder home page will be loaded automatically after restart is completed.

This completes the configuration of the RF550VPN/RF560VPN at Site A. Now configure the NAT box and SSH Sentinel client at Site B.

Example 1: NAT Box Configuration at Site B

Configure the NAT box for IPSec Pass-Through by specifying the IP address and subnet mask assigned by the ISP for Site B (Ex: 204.26.122.3). Then specify the ISP Gateway Address. (Ex: 204.26.122.103)

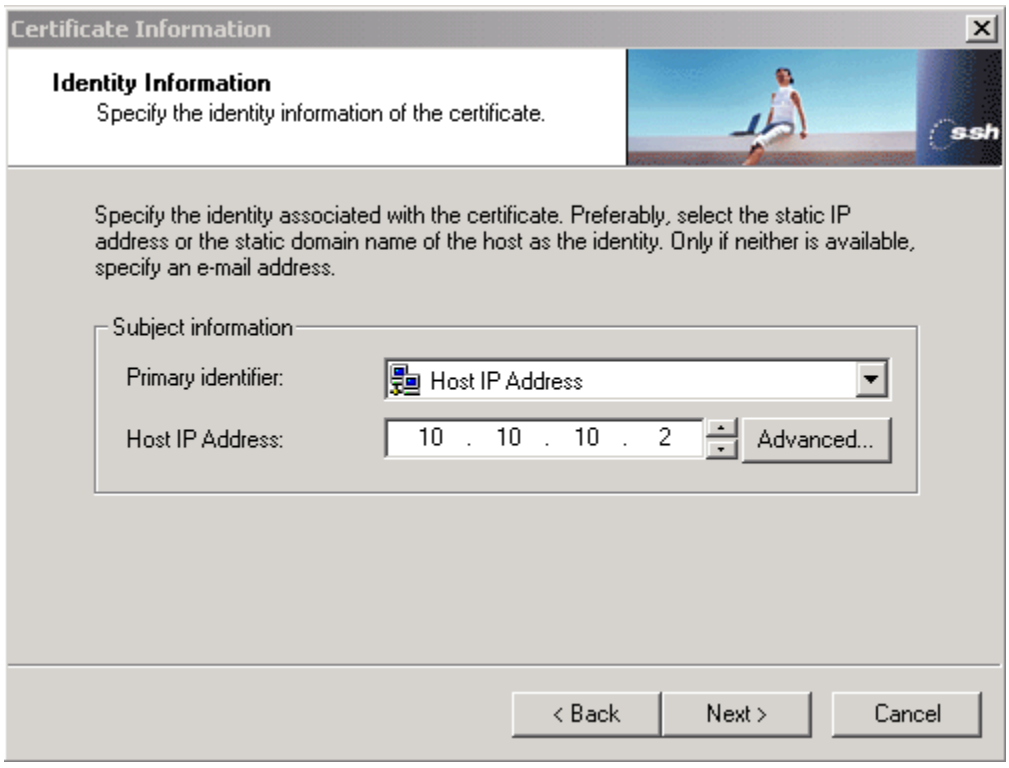
Screen shot for the RF500S:


CABLE/xDSL ISP SETTINGS
Your ISP requires you to input IP settings
IP assigned by your ISP: 204 . 26 . 122 . 3
IP Subnet Mask: 255 . 255 . 255 . 0
ISP Gateway Address: 204 . 26 . 122 . 103
Domain Name Server (DNS) IP Address: 0 . 0 . 0 . 0

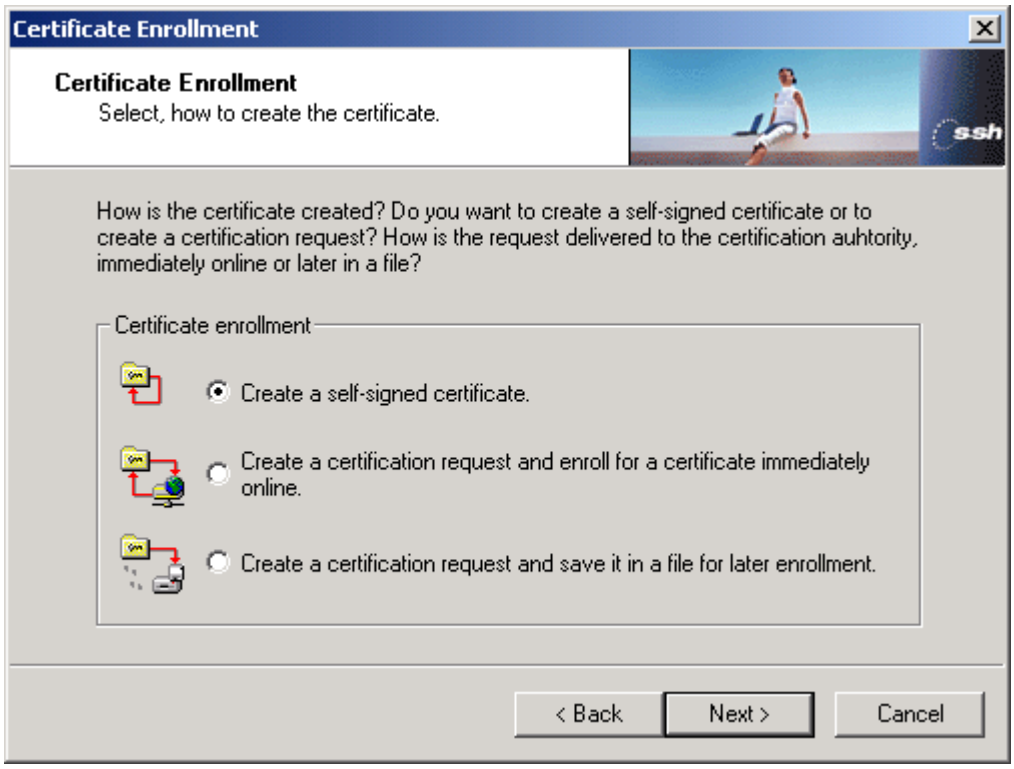
Example 1: SSH Sentinel 1.3 Client Configuration Procedure at Site B

Note: This example will install and run SSH Sentinel version 1.3 on Windows 2000 Professional. For Sentinel 1.4 see the Sentinel 1.4 Reference Guide on the Multi-Tech Web Site.

1. Before installing version 1.3 of SSH Sentinel, be sure to uninstall all other versions of IPSec client.
2. Install the Sentinel IPSec client using the **InstallShield Wizard** and select all the defaults as you move through the setup screens.
3. Click **Next** on the **Welcome** screen.
4. Click **Yes** for the license agreement.
5. Click **Next** to use the default installation destination path.
6. Click **Next** to display the default program folder.
7. Sentinel will now install.
8. On the next screen move the mouse around to generate a host authentication **keypair**. When complete, click **Next**.
9. At the **Authentication Key Information** Screen select the **Host IP Address** for the **Primary Identifier**. Then the IP Address for the Windows 2000 system appears in the **Host IP Address** window. (Ex: 10.10.10.2)


Certificate Information
Identity Information
Specify the identity information of the certificate.
ssh
Specify the identity associated with the certificate. Preferably, select the static IP address or the static domain name of the host as the identity. Only if neither is available, specify an e-mail address.
Subject information
Primary identifier:
Host IP Address
Host IP Address:
10 . 10 . 10 . 2
Advanced...
< Back
Next >
Cancel

10. At the **Certificate Enrollment Method** screen select the default choice of **Create a self-signed certificate**.


Certificate Enrollment
Certificate Enrollment
Select, how to create the certificate.
ssh
How is the certificate created? Do you want to create a self-signed certificate or to create a certification request? How is the request delivered to the certification auhtority, immediately online or later in a file?
Certificate enrollment
Create a self-signed certificate.
Create a certification request and enroll for a certificate immediately online.
Create a certification request and save it in a file for later enrollment.
< Back
Next >
Cancel

11. Now the **Encryption Speed Diagnostics** screen is displayed. You have the option of skipping this test. Click on **Skip** or wait until the diagnostic has finished and click on **Next**.

12. Click on **Finish** and allow the system to reboot.

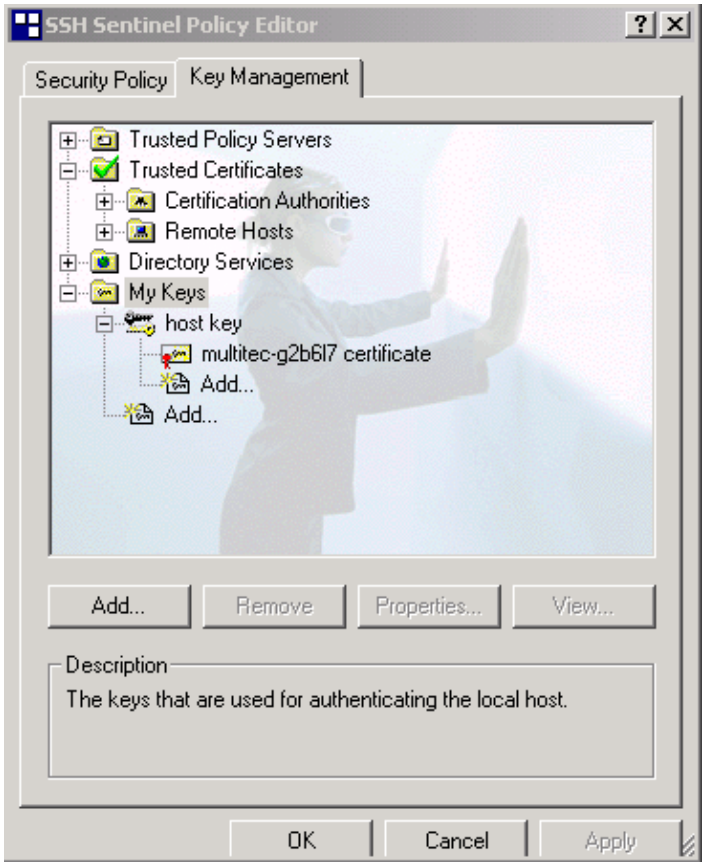
SSH Sentinel Installation
ssh
SSH Sentinel installation completed
The software is successfully installed. The modification made to the operating system kernel are not put into effect before you restart your computer.
Would you like to restart your computer?
Yes, restart the computer.
No, I will restart at a later time.
Please remove any disks from their drives, and click Finish to complete setup.
< Back
Finish
Cancel

13. Once Windows has rebooted, right click on the SSH icon at the bottom right-hand corner of your screen.

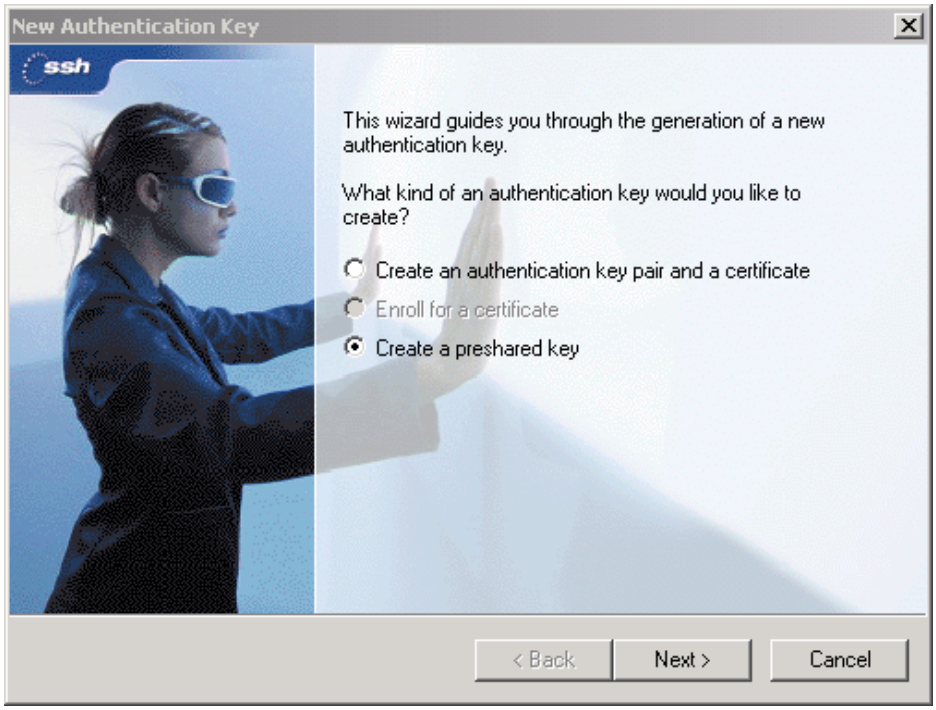
^

14. Select **Run Policy Editor**.

15. Click on the **Key Management** tab at the top of the SSH window.
16. Highlight **My Keys** and click on **Add** to create a new Authentication Key.



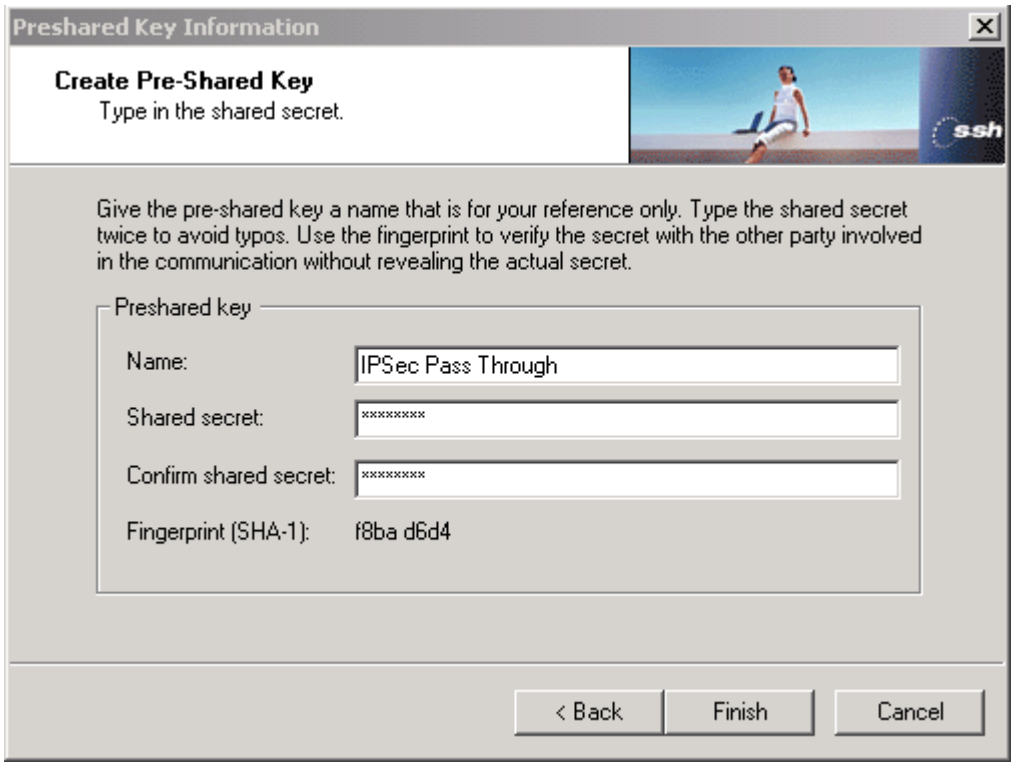
17. Check the **Create a preshared key** checkbox and click **Next**.


New Authentication Key
ssh
This wizard guides you through the generation of a new authentication key.
What kind of an authentication key would you like to create?
Create an authentication key pair and a certificate
Enroll for a certificate
Create a preshared key
< Back
Next >
Cancel

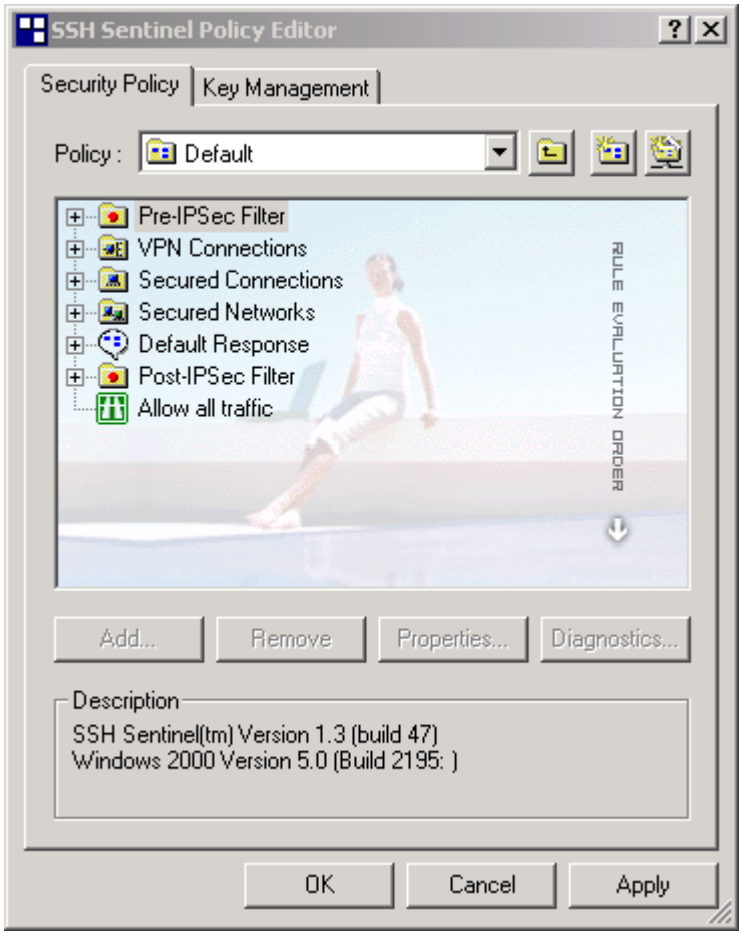
18. Enter the **Preshared key information** and click on **Finish**. The **Shared secret** needs to match what was entered at Site A for the RF550VPN/RF560VPN configuration in step 9.

    Key name = IPSec Pass Through
    Shared secret = 1o2t3t4f

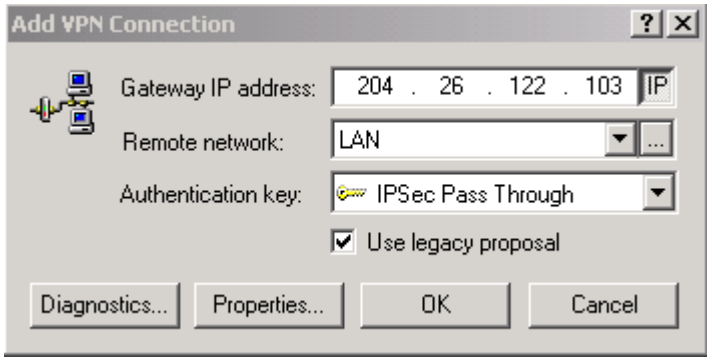
19. Click on **Finish**.


Preshared Key Information
Create Pre-Shared Key
Type in the shared secret.
ssh
Give the pre-shared key a name that is for your reference only. Type the shared secret twice to avoid typos. Use the fingerprint to verify the secret with the other party involved in the communication without revealing the actual secret.
Preshared key
Name:
IPSec Pass Through
Shared secret:
****
Confirm shared secret:
****
Fingerprint (SHA-1):
f8ba d6d4
< Back
Finish
Cancel

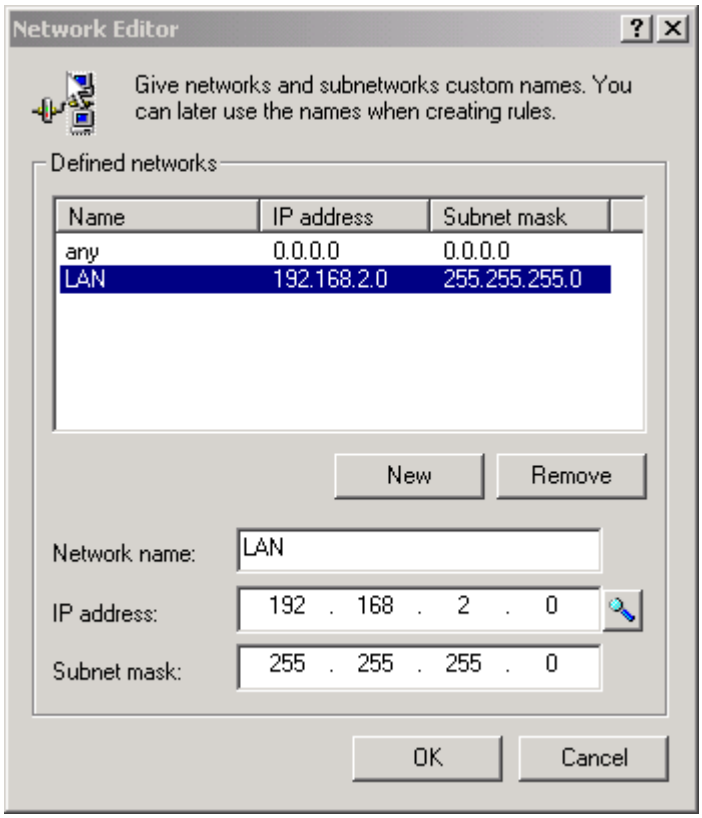
20. Click on **Apply** and then the **Security Policy** tab at the top, double click **VPN Connection** and click **add**.



21. At the **Add VPN Connection** screen enter the **Security Gateway** information. Click on **IP** and enter the public (WAN) IP address of the RF550VPN/RF560VPN at Site A (204.26.122.103). Click on the down arrow for the **Authentication key** and select the key name that was created in step 18(IPSec Pass Through). Check the box for **Use Legacy Proposal.**

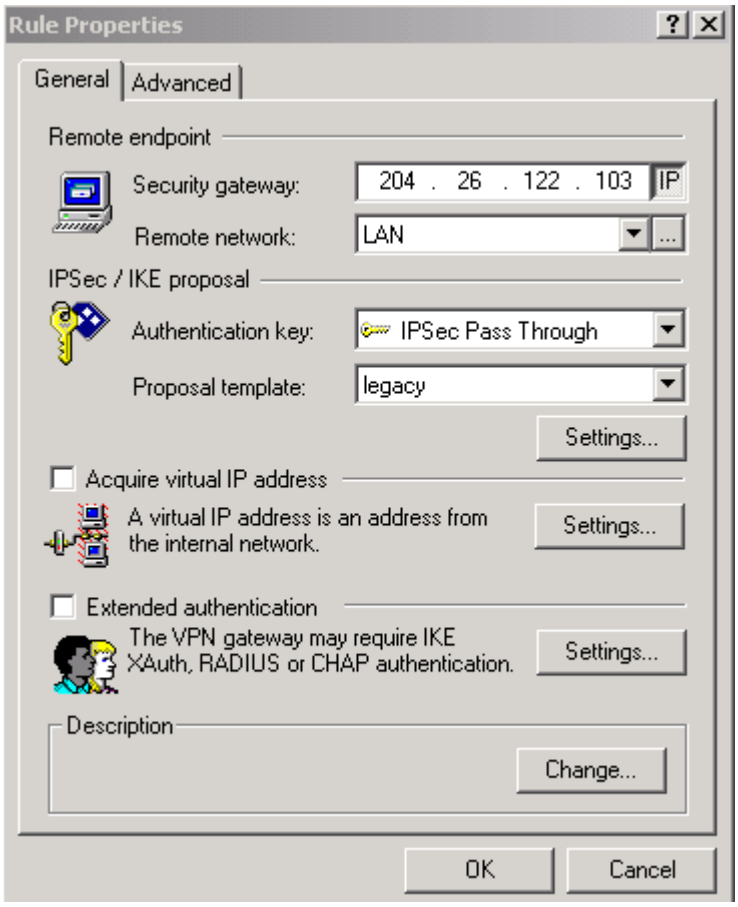


22. Click on **… ,** click on **New**, enter the **Network name**, the **IP address** and the **Subnet mask** for the LAN side of the RouteFinder. (Ex: LAN, 192.169.2.0, 255.255.255.0) Then click **OK** at the **Network Editor** screen and then click **OK** again at the **Add VPN Connection** screen.



23. Now back at the **Policy Editor** screen, highlight the connection you just created (204.26.122.103) and click on **Properties**.

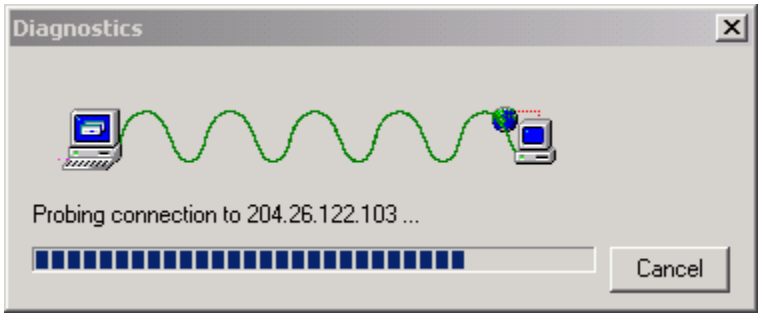
24. The **Connection Properties** | **General** screen is displayed. Click on **Settings…** under **IPSec / IKE proposal** and verify that the **PFS Group** is set to **Group 2**. Click on **OK**.



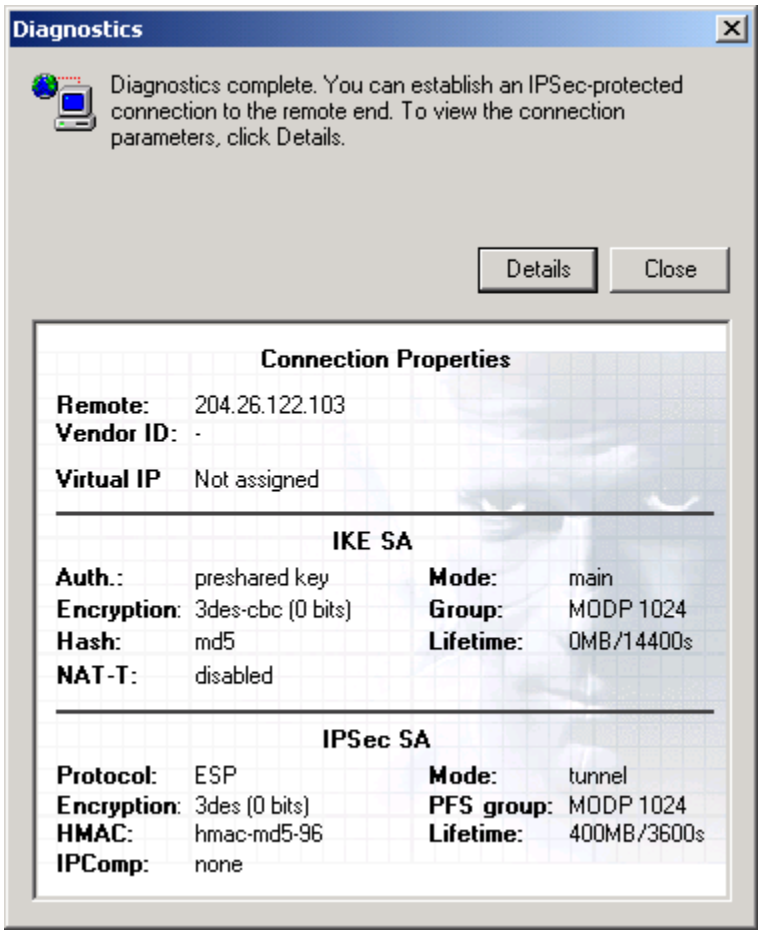
25. Click on the **Advanced** tab. Check the box for **Open on start-up**. Then click on **OK** to close the **Rule Properties** screen.

26. Now back at the **Policy Editor** screen, click on **Apply**, and then click twice on **VPN Connection**. Highlight the connection you just created (204.26.122.103) and click on **Diagnostics**.

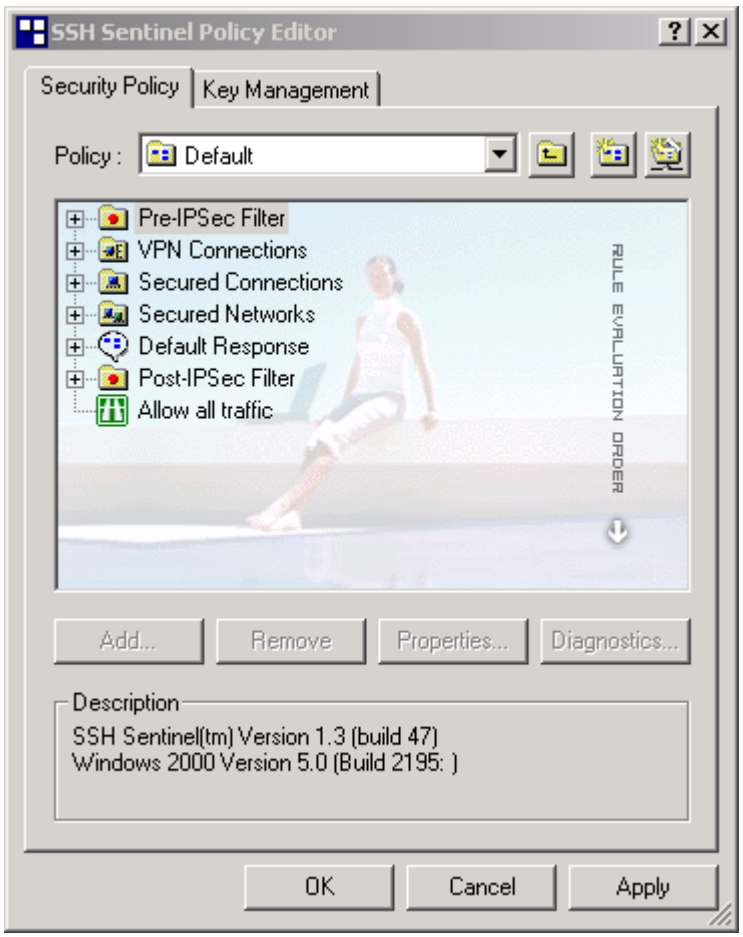
27. Sentinel will probe for a connection to the RF550VPN/RF560VPN and should be successful.



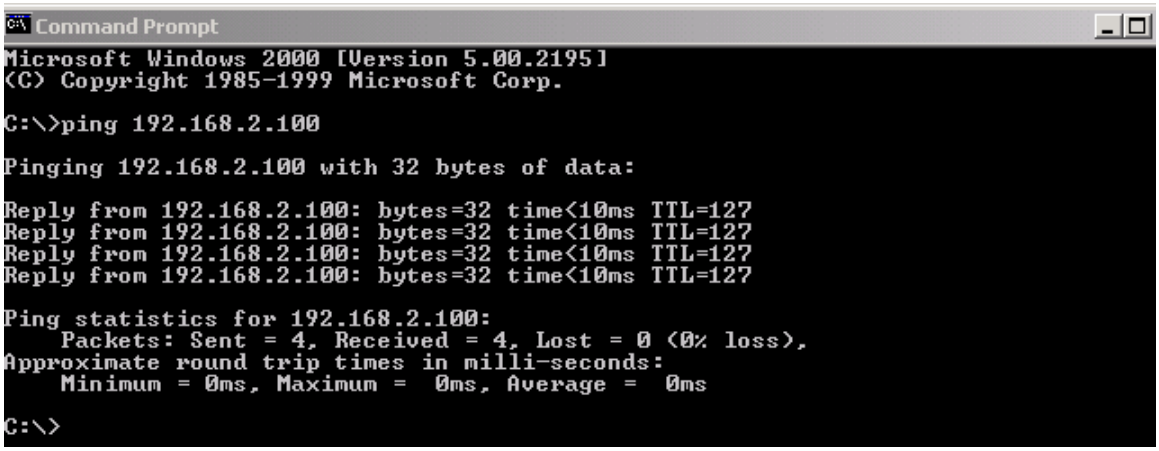
28. Click **Details**. Details of the newly created connection are displayed.



29. Verify the connection details information and click **Close**.



30. Click **OK** to close the SSH Sentinel window.
31. Open a DOS command prompt window and attempt to **PING** the LAN located behind the RF550VPN/RF560VPN. If the **PING** is successful, the configuration process to connect SSH Sentinel client to an RF550VPN/RF560VPN RouteFinder is complete. If **PING** fails, stop and restart the Sentinel Policy Manager. If still fails, check cabling and software configuration at both locations.

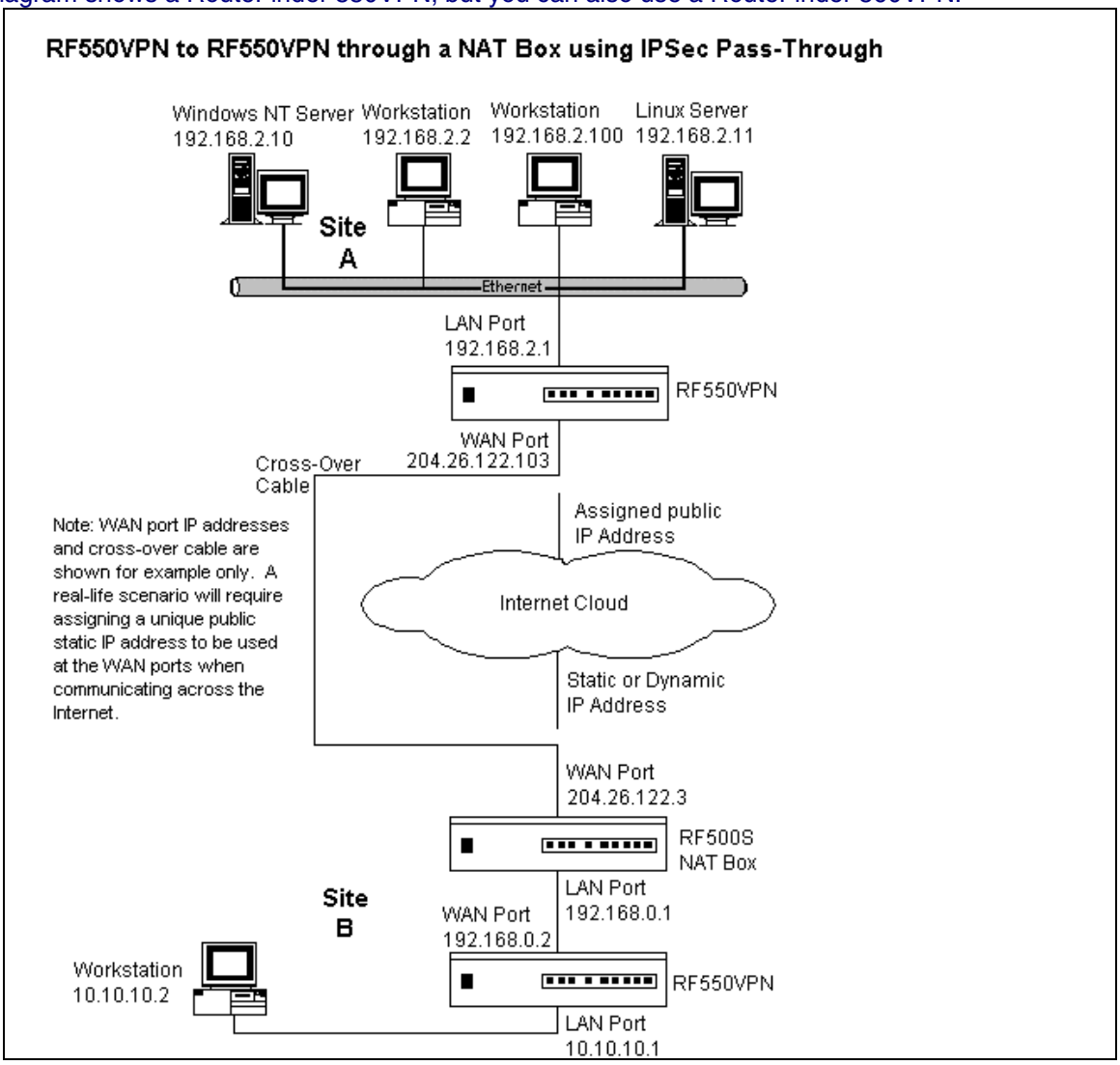


Note: The Sentinel Policy Manager may need to be stopped and started in order for you to successfully **PING** the remote LAN. Once you can **PING** the remote LAN, do not run the diagnostics test again, otherwise, you will have to stop and start the policy manager in order to once again **PING** successfully.

Example 2

This example provides a sample RouteFinder configuration and related address scheme for an application employing LAN-to-LAN IPSec Pass-Through communication. This is an example on how to configure an RF550VPN/RF560VPN at Site A and an RF550VPN/RF560VPN behind a NAT box at Site B, so Site A and B can communicate through a secure connection over the Internet using IPSec Pass-Through. This example deals with Site B using a static and dynamic IP address.

The diagram shows a RouteFinder 550VPN, but you can also use a RouteFinder 560VPN.


RF550VPN to RF550VPN through a NAT Box using IPSec Pass-Through
Windows NT Server 192.168.2.10
Workstation 192.168.2.2
Workstation 192.168.2.100
Linux Server 192.168.2.11
Site A
Ethernet
LAN Port 192.168.2.1
RF550VPN
WAN Port 204.26.122.103
Cross-Over Cable
Note: WAN port IP addresses and cross-over cable are shown for example only. A real-life scenario will require assigning a unique public static IP address to be used at the WAN ports when communicating across the Internet.
Assigned public IP Address
Internet Cloud
Static or Dynamic IP Address
WAN Port 204.26.122.3
RF500S NAT Box
Site B
LAN Port 192.168.0.1
WAN Port 192.168.0.2
Workstation 10.10.10.2
RF550VPN
LAN Port 10.10.10.1

Note: Make sure that all routers between both SSH IPSec ends can route IP protocol 50 (IPSec). Sometimes routers are configured to route only TCP (protocol 6), UDP (protocol 17) and ICMP (Protocol 1) and drop all other protocols. VPN routers configured that way won't work with IPSec!

Example 2: LAN-to-LAN Configuration Chart

LAN-to-LAN Application – Site A: RF550VPN/RF560VPN	LAN-to-LAN Application – Site B: RF550VPN/RF560VPN
1. Domain name = Site-A.com 2. Public Class C = 204.26.122.x 3. SETUP WIZARD > DEVICE IP SETTINGS IP Address: 192.168.2.1 IP Subnet Mask: 255.255.255.0 4. SETUP WIZARD > ISP SETTINGS Select “Static IP Settings’ IP assigned by your ISP: 204.26.122.103 IP Subnet Mask: 255.255.255.0 ISP Gateway Address: 204.26.122.3 5. SETUP WIZARD > VPN SETTINGS Connection Name = Site-B Enable ‘Enable UID (Unique Identifier String) Local IPSEC Identifier = 204.26.122.103 Remote IPSEC Identifier = 192.168.0.2 Disable (do not check) ‘Enabled Keep Alive’ Disable (do not check) ‘Enabled NetBIOS Broadcast’ Remote Site = LAN Remote IP Network = 10.10.10.0 Remote IP Netmask = 255.255.255.0 Remote Gateway IP = 204.26.122.3 Network Interface = WAN ETHERNET Secure Association = check ‘IKE’ Perfect Forward Secure = check ‘enabled’ Encryption Protocol = select ‘3DES’ Preshared Key (must match secret code at Site B) Key Life = set to default IKE Life Time = set to default	1. Domain name = Site-B.com 2. Public Class C = 204.26.122.x 3. SETUP WIZARD > DEVICE IP SETTINGS IP Address: 10.10.10.1 IP Subnet Mask: 255.255.255.0 4. SETUP WIZARD > IISP SETTINGS Select “Static IP Settings’ IP assigned by your ISP: 192.168.0.2 IP Subnet Mask: 255.255.255.0 ISP Gateway Address: 192.168.0.1 5. SETUP WIZARD > VPN SETTINGS Connection Name = Site-A Enable ‘Enable UID (Unique Identifier String) Local IPSEC Identifier = 192.168.0.2 Remote IPSEC Identifier = 204.26.122.103 Disable (do not check) ‘Enabled Keep Alive’ Disable (do not check) ‘Enabled NetBIOS Broadcast’ Remote Site = LAN Remote IP Network = 192.168.2.0 Remote IP Netmask = 255.255.255.0 Remote Gateway IP = 204.26.122.103 Network Interface = WAN ETHERNET Secure Association = check ‘IKE’ Perfect Forward Secure = check ‘enabled’ Encryption Protocol = select ‘3DES’ Preshared Key (must match secret code at Site A) Key Life = set to default IKE Life Time = set to default

Software Configuration

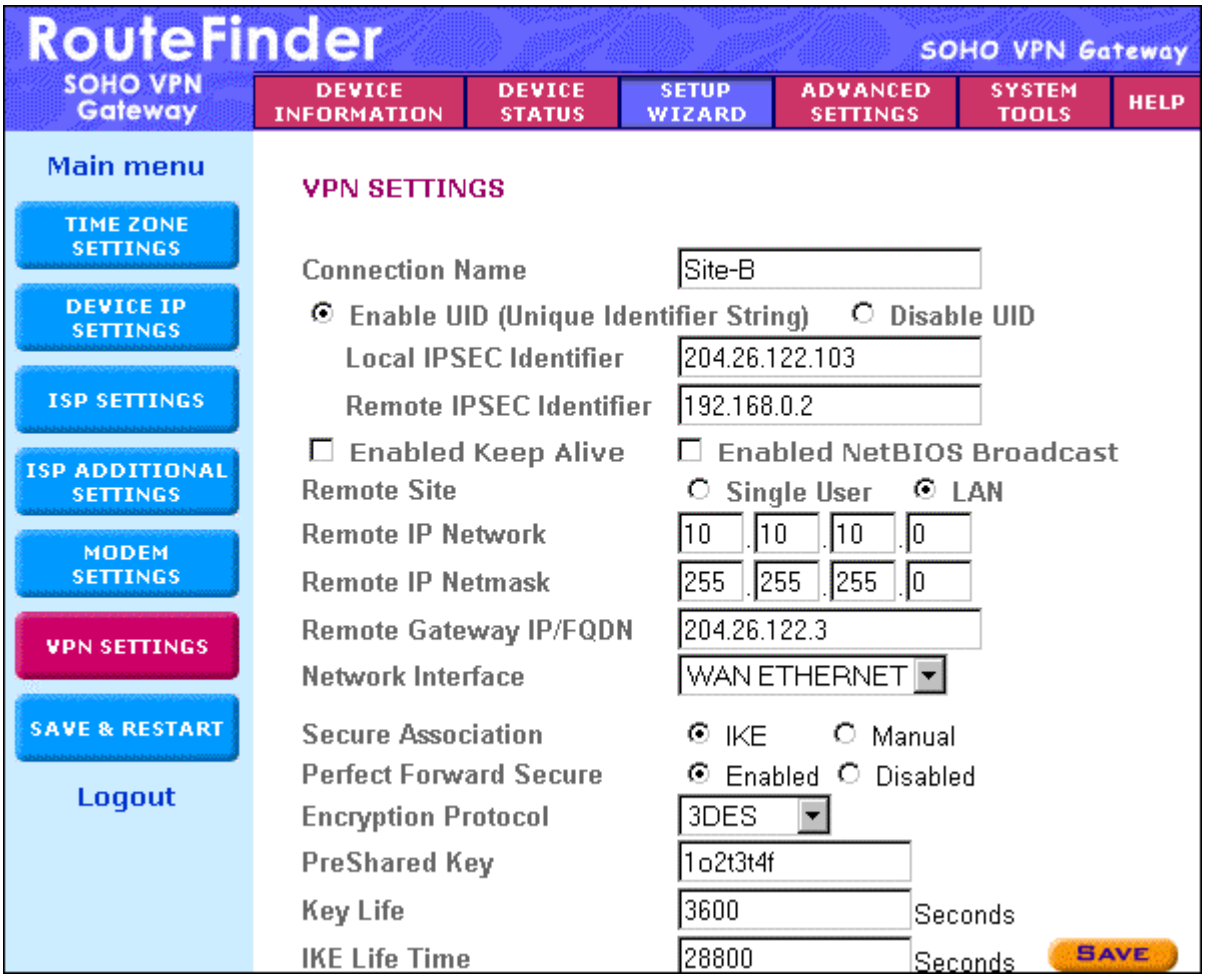
Example 2: Configuration Procedure at Site A

Note: To configure the RF550VPN/RF560VPN at Site A follow the same procedure as in example 1, **but change the following items in the RF550VPN/RF560VPN configuration:**

1. Click the button on the left side of the screen for **VPN Settings**. Use this screen to setup your LAN-to-LAN VPN connection.

2. In the **Connection Name** field, type a name that identifies for you a connection that you would like to make. (Ex: **Site-B**) Click the **Add** button.

3. The **VPN Settings** screen for entering specific VPN settings will display. The **Connection Name** (**Site-B**) defaults into the first field. Enter the following settings:



a) Select **Enable UID**.

b) **Local IPSec Identifier –** Enter an IP address that identifies the Local IPSec for this connection. (Ex: **204.26.122.103**)

c) **Remote IPSec Identifier –** Enter an IP address that identifies the Remote IPSec for this connection. (Ex: **192.168.0.2**)

d) **Remote IP Network –** Enter the **Remote IP Network** address (**LAN**) for Site B. (Ex: **10.10.10.0**)

e) **Remote IP Netmask –** Enter the **Remote IP Netmask** address for Site B. (Ex: **255.255.255.0**)

f) **Remote Gateway IP –** Enter the **Remote Gateway IP** address (**WAN**) for Site B. (Ex: **204.26.122.3**) If Site B is using dynamic IP addressing, set this value to 0.0.0.0.

g) **Network Interface –** Select the **Network Interface** from the drop-down list box. (Ex: **WAN Ethernet**)

h) **Secure Association –** Select **IKE** to set how inbound packets will be filtered. **IKE** is the default. **IKE** primarily encompasses router key exchange and the negotiation of security policy. Selecting **IKE** displays field h-l.

i) **Perfect Forward Secure –** Check the **Enabled** button.

j) **Encryption Protocol** – Select the encryption protocol used for your configuration. The default protocol for the RF550VPN/RF560VPN communicating with another RF550VPN/RF560VPN is **3DES**. (Ex: **3DES**)

k) **PreShared Key –** Enter the **PreShared Key** name (you can enter an alphanumeric name but it needs to match the security code for the RouteFinder at Site B).

l) **Key Life –** Enter the amount of time that tells the router to renegotiate the Key. For example, 3600 seconds is 60 minutes.

m) **IKE Life Time –** Enter the amount of time that tells the router to renegotiate the IKE security association. For example, 28800 seconds is 8 hours.

4. Click the **Save** button. The data entered on this screen will be displayed on the VPN Settings screen where you can enable/disable, edit or delete them. To enable this connection, check the **Enable** box that appears to the left of the connection name.

5. Save and restart the RouteFinder.

This completes the configuration of the RF550VPN/RF560VPN at Site A.

Example 2: NAT Box Configuration at Site B

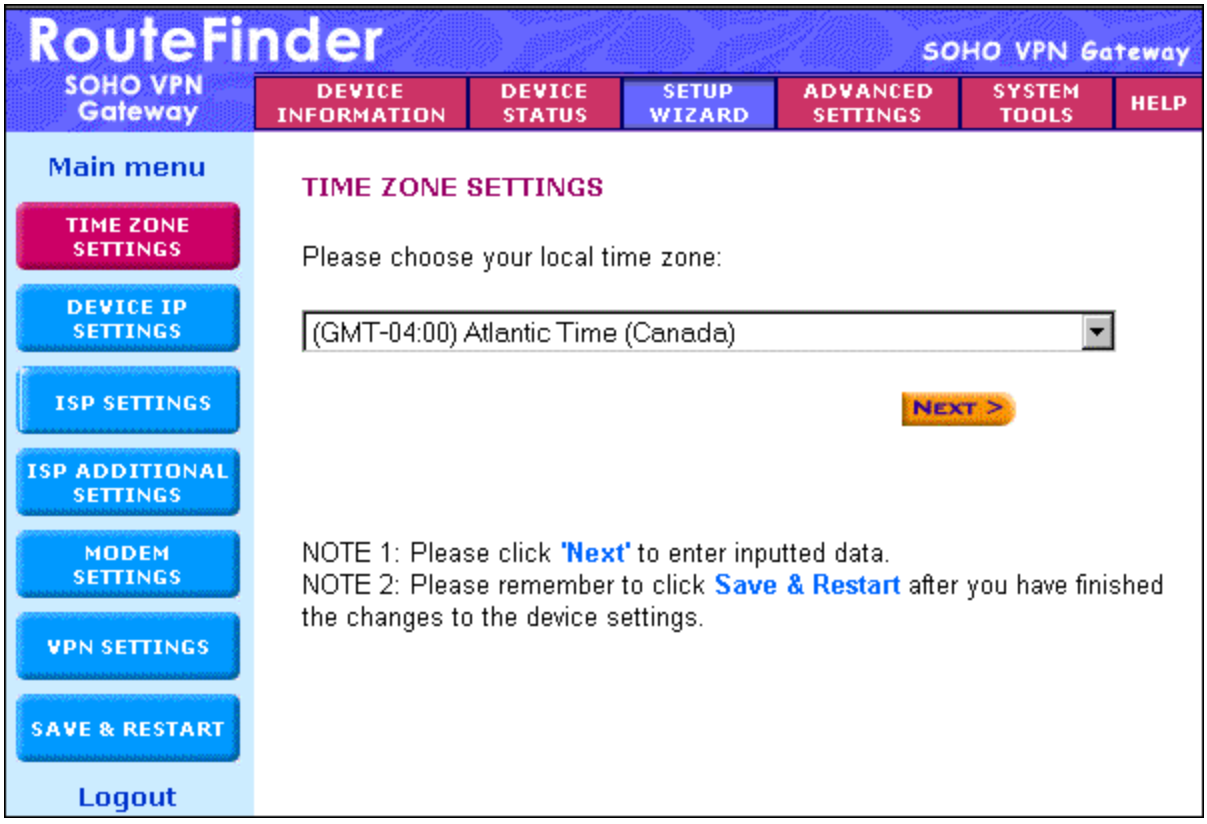
Configure the NAT box for IPSec Pass-Through by specifying the IP address and subnet mask assigned by the ISP for Site B (Ex: 204.26.122.3). Then specify the ISP Gateway Address. (Ex: 204.26.122.103) **This is the same as the NAT box in example 1, but for this example, the LAN connection needs to be set to 192.168.0.1**

Example 2: RF550VPN/RF560VPN Configuration at Site B

1. Connect a workstation to one of the RF550VPN/RF560VPN's **LAN ports** via Ethernet for Site B.

   Note: It is assumed that the IP Address of the RouteFinder's **LAN** at Site B (Ex: 10.10.10.1) has already been changed from it's default (192.168.2.1) so it does not conflict with the IP Address of the RouteFinder's **LAN** at Site A (Ex: 192.168.2.1).
2. Set the workstation IP address to 10.10.10.x subnet.
3. Apply power to the RF550VPN/RF560VPN RouteFinder and allow the LEDs to stabilize on the unit.
4. Bring up your Web browser on the workstation. At the browser's address line, type the Gateway address of http://10.10.10.1 and press the Enter key.
5. After typing the IP Address in the web browser, the RF550VPN/RF560VPN main menu displays.
6. On the Main Menu, click the **Setup Wizard** button. The **Password** dialog box displays.
7. Type **admin** (**admin** is the default user name) in the user name box and leave the password box empty.

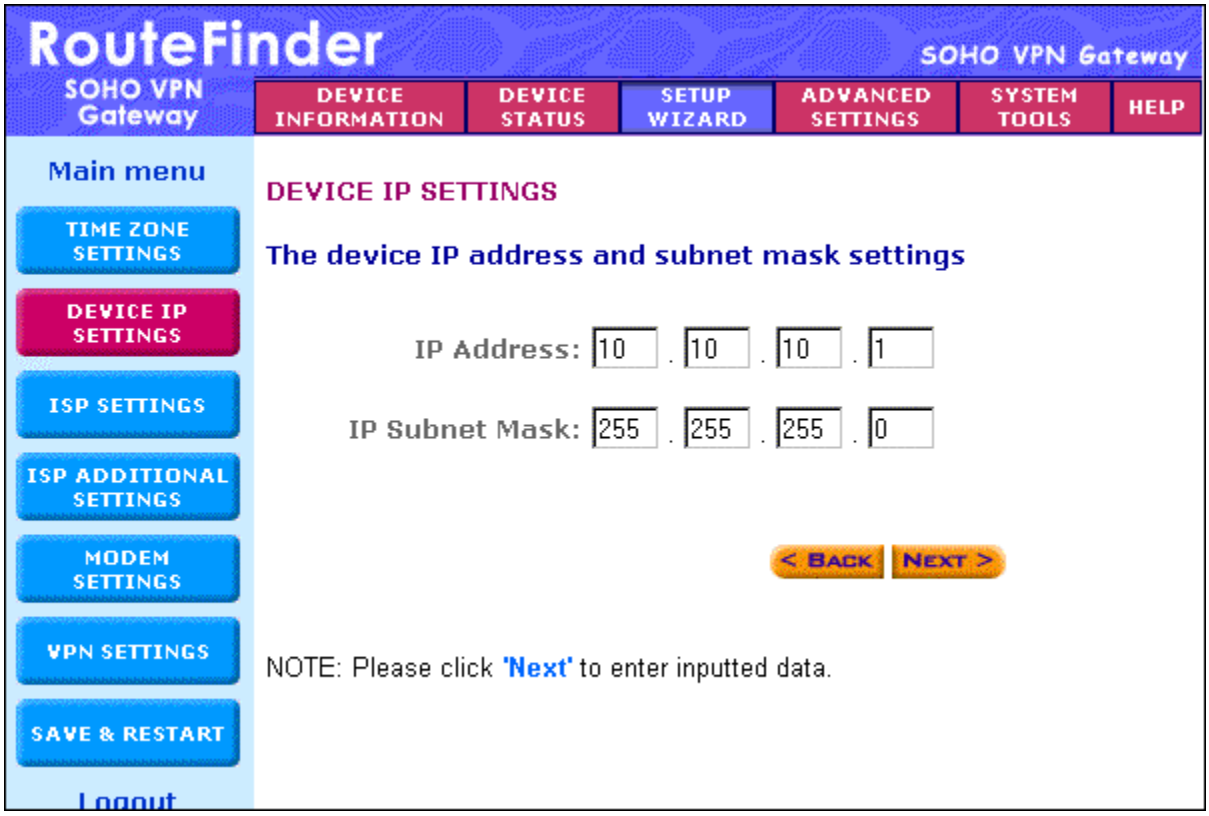
   Note: To change your password after logging in, select the **Advanced Settings** button and **Administrative Settings**.
8. Click **OK**. The **Setup Wizard** screen displays a step-by-step process that lets you input all of the basic settings to configure your RF550VPN/RF560VPN.
9. Select the **Time Zone**, and then click the **Next** button to continue.



10. For **Device IP Settings** enter the internal LAN IP address and subnet mask that you want assigned to the LAN ports of the RF550VPN/RF560VPN. This is not the IP address from your ISP but the local internal LAN IP address. The default IP address is **192.168.2.1** but for our example we will use **10.10.10.1**.

    Device IP Address: 10.10.10.1.
    Device IP Subnet Mask: 255.255.255.0

    Click the **Next** button.



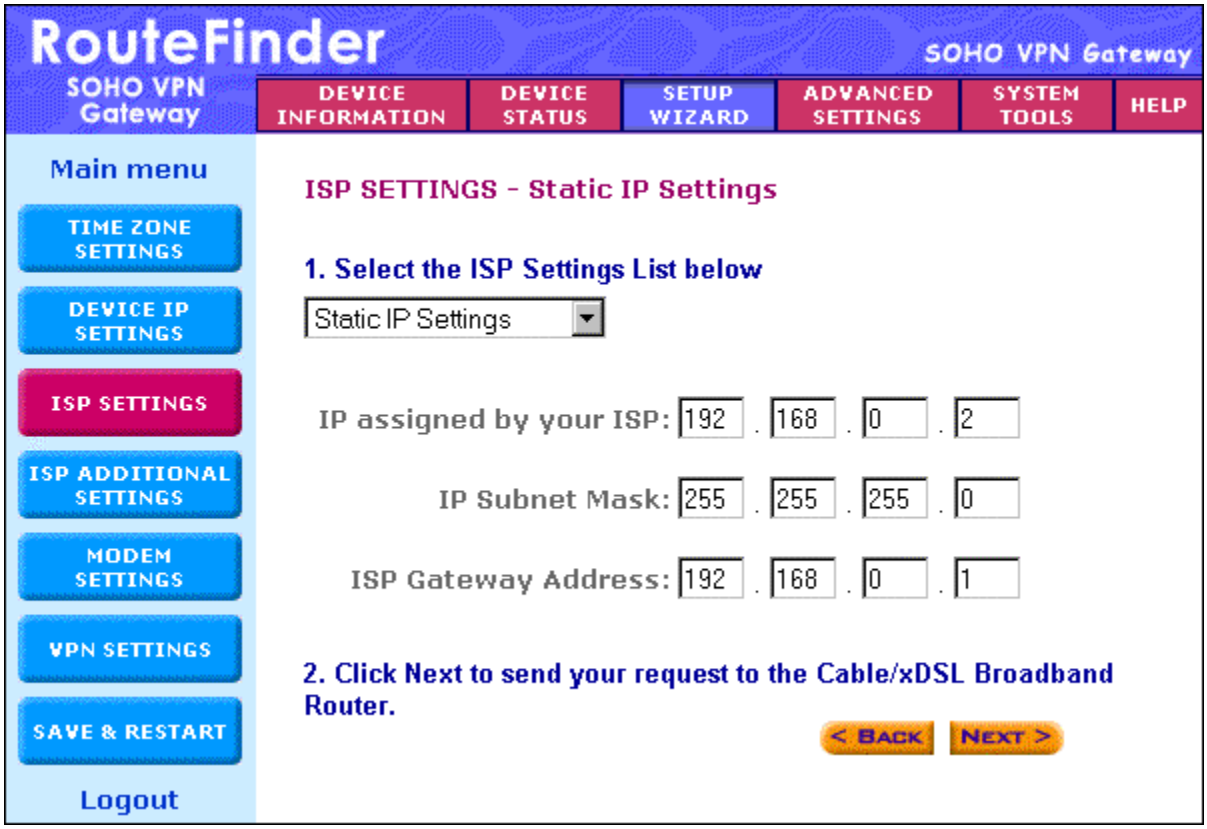
11. Select **Static IP Settings** and enter the following information.

    a) **IP Assigned by your ISP:** This is the IP address of the WAN port on the RF550VPN/RF560VPN at Site B.
    (Ex: 192.168.0.2)

    b) **IP Subnet Mask:** This is the IP address of the subnet mask for the WAN port on the RF550VPN/RF560VPN at Site B. (Ex: 255.255.255.0)

    c) **IP Gateway Address:** This is the IP address of the LAN port on the RF500S NAT Box at Site B. (Ex: 192.168.0.1)

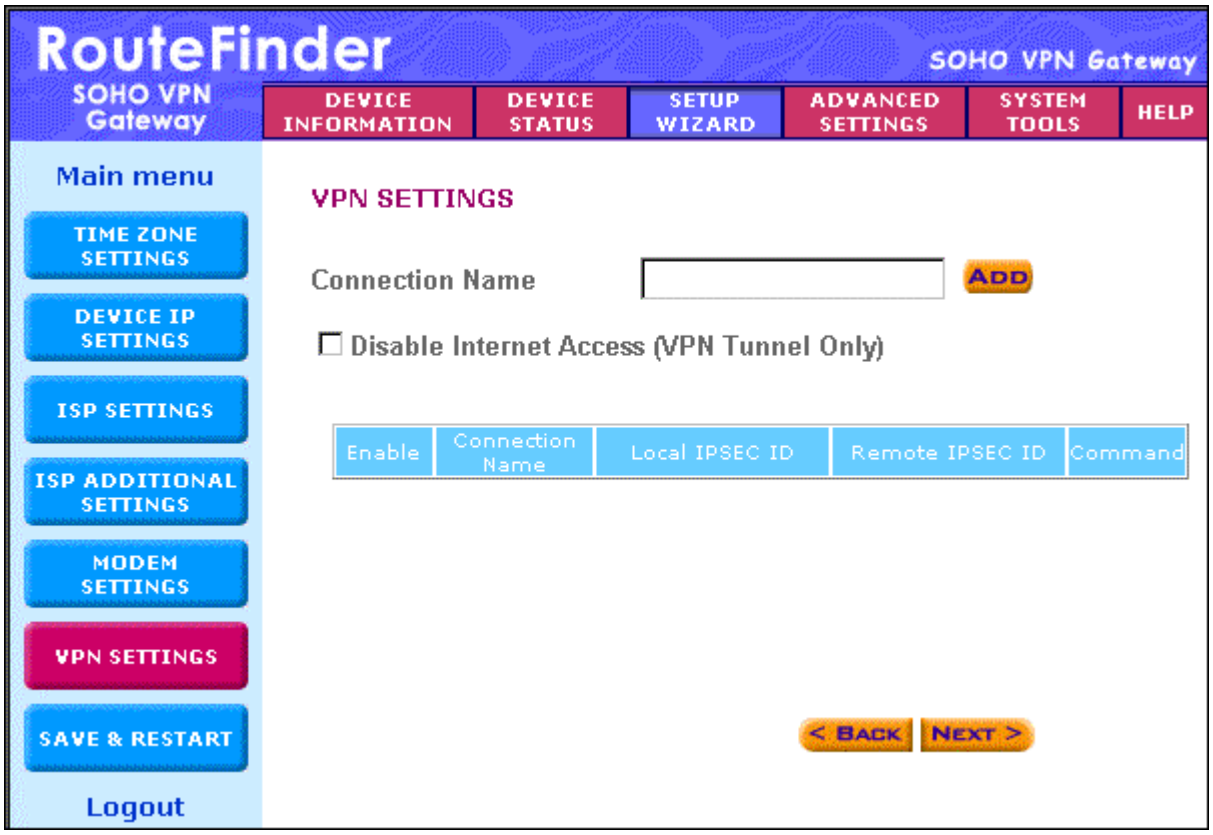
    Click the **Next** button.


RouteFinder
SOHO VPN Gateway
SOHO VPN Gateway
DEVICE INFORMATION
DEVICE STATUS
SETUP WIZARD
ADVANCED SETTINGS
SYSTEM TOOLS
HELP
Main menu
TIME ZONE SETTINGS
DEVICE IP SETTINGS
ISP SETTINGS
ISP ADDITIONAL SETTINGS
MODEM SETTINGS
VPN SETTINGS
SAVE & RESTART
Logout
ISP SETTINGS - Static IP Settings
1. Select the ISP Settings List below
Static IP Settings
IP assigned by your ISP: 192 . 168 . 0 . 2
IP Subnet Mask: 255 . 255 . 255 . 0
ISP Gateway Address: 192 . 168 . 0 . 1
2. Click Next to send your request to the Cable/xDSL Broadband Router.
< BACK
NEXT >

Note: For this scenario of connecting two RouteFinders back-to-back it is not necessary to enter any information for the **ISP Additional Settings** or **Modem Settings**.

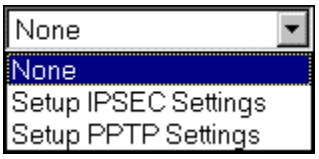
12. Click the button on the left side of the screen for **VPN Settings**. Use this screen to setup your LAN-to-LAN VPN connection.

13. **For RF550VPN:** In the **Connection Name** field, type a name that identifies for you a connection that you would like to make. (Ex: **Site-A**). Click the **Add** button.

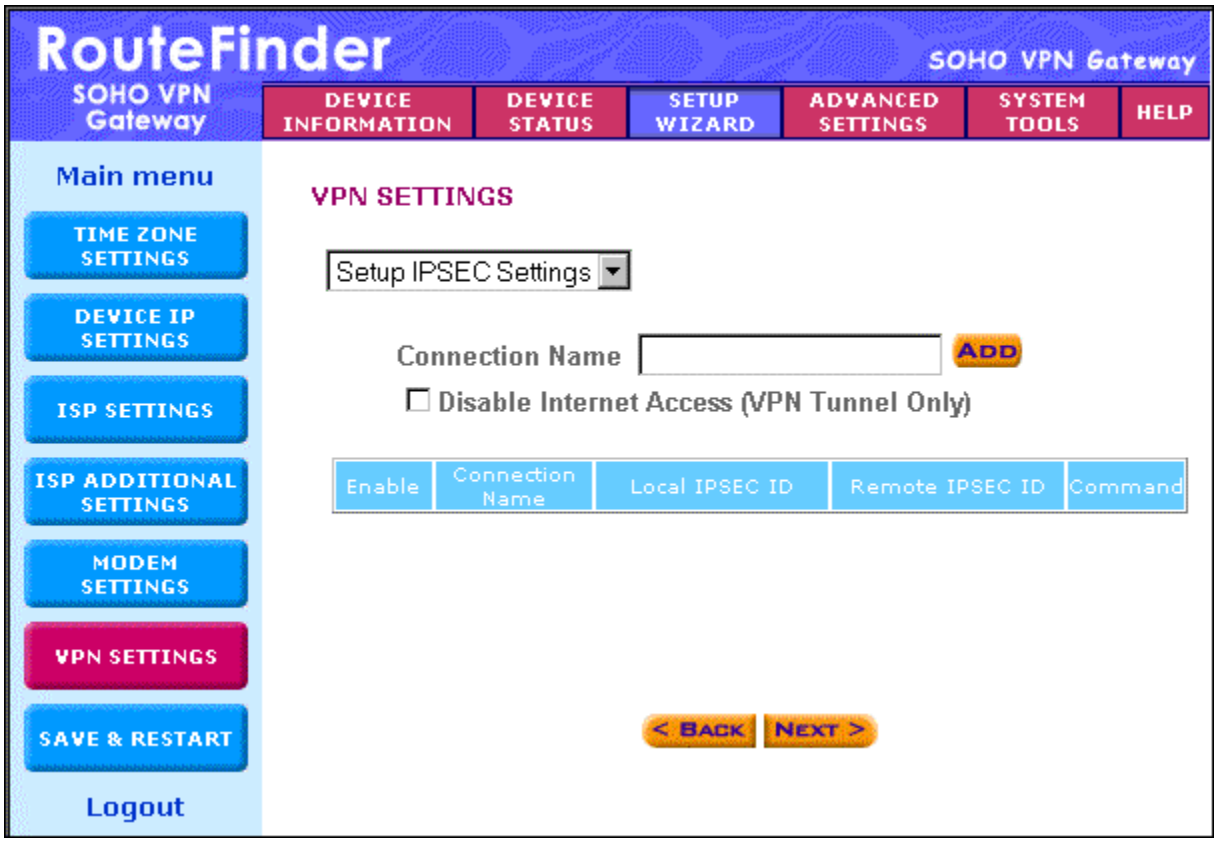


For the RF560VPN:

From the **VPN Settings** drop-down list box, select the type of VPN Connection you want to set:



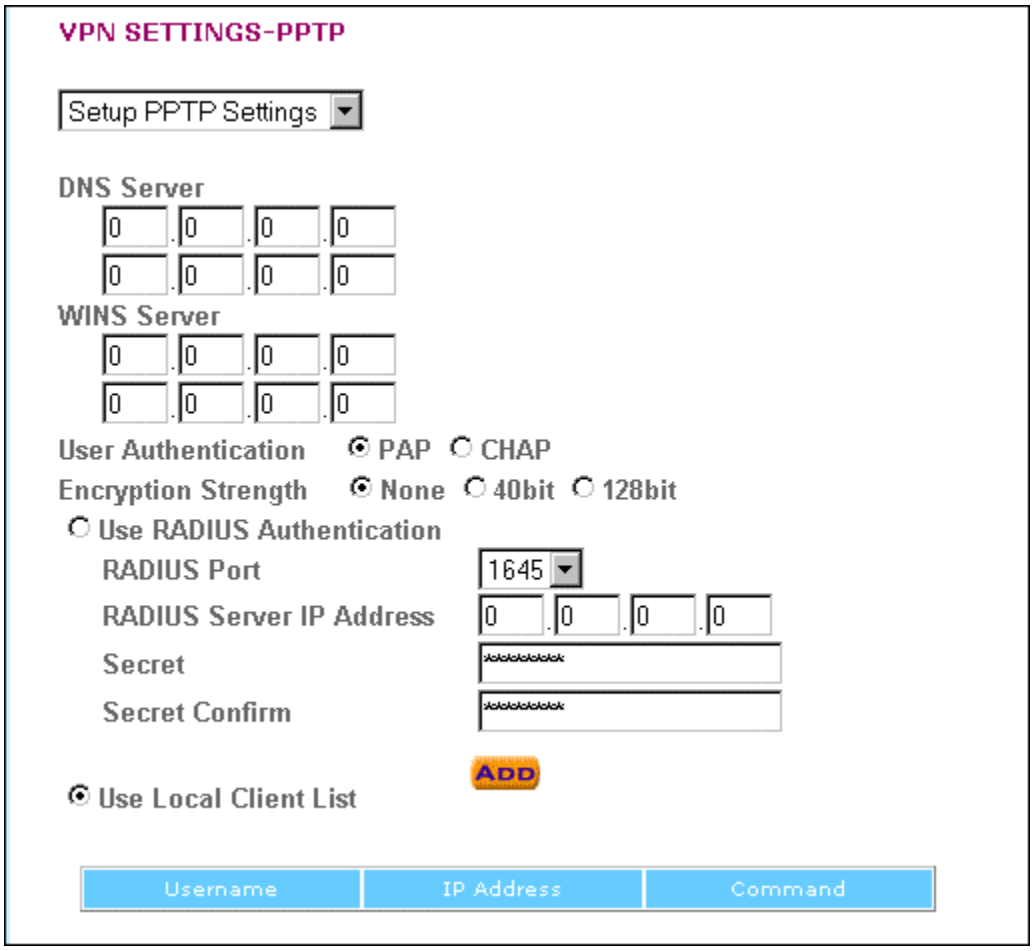
If you select Setup IPSEC Settings, the following screen displays:



- In the **Connection Name** field, type a name that describes a connection you would like to make.
- Example: **Site A**.
- Click the **Add** button, and the **VPN Settings** detail screen will display (see the next screen). Once you have entered the settings, the **Connection Name** displays on the lower half of the screen (above).
- Click the checkbox if you want to **Disable Internet Access (VPN Tunnel Only).**
- You can then edit, delete, or enable/disable this connection by clicking the corresponding buttons.
- To enable this connection, check the **Enable** box.

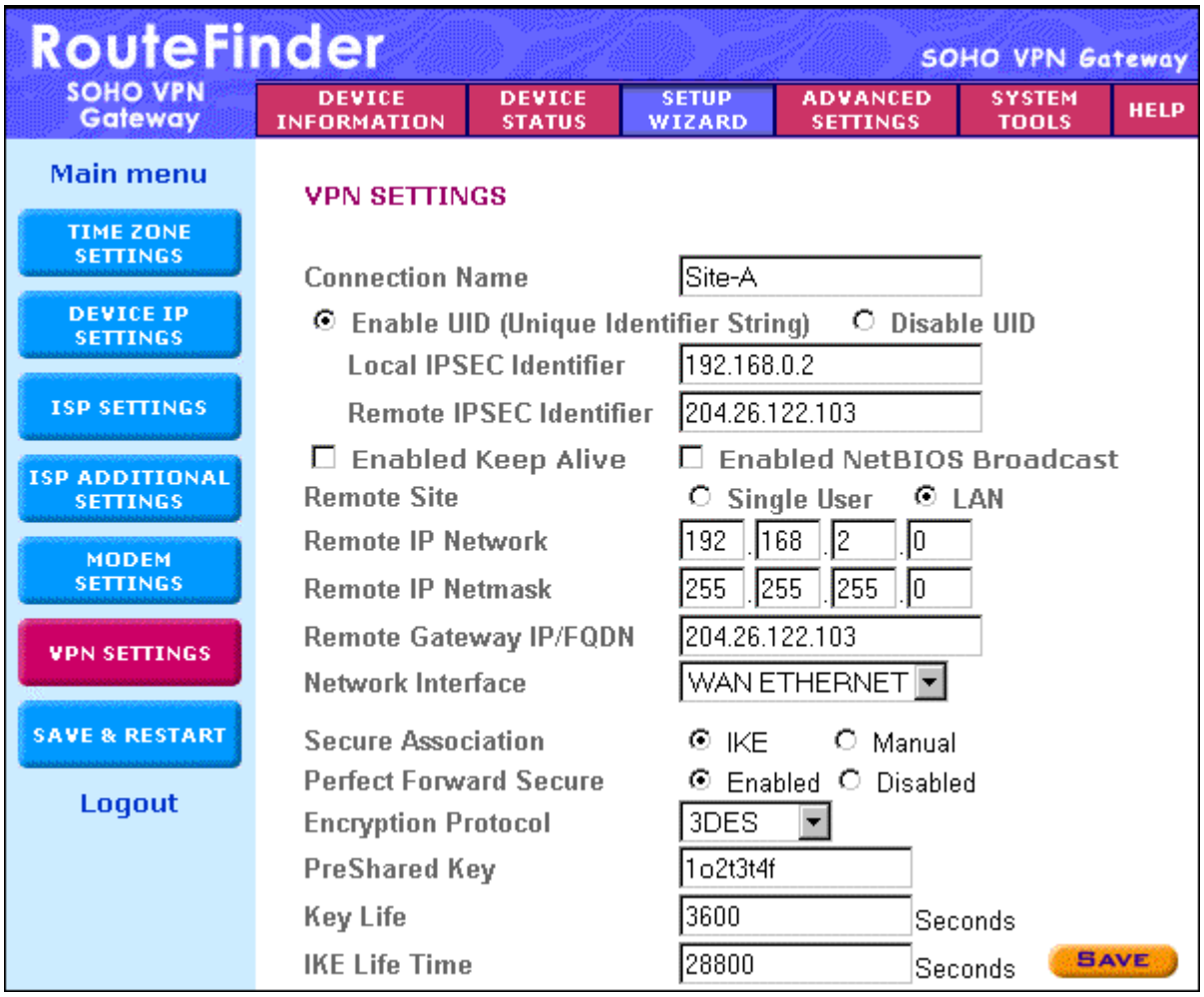
Note: If you uncheck the **Enable** box, the connection will not be active, but the parameters will remain on the screen for you to enable, edit, or delete as desired.

If you select Setup PPTP Settings, the following screen displays:



- **DNS Server** – Enter the address of the DNS Server to be used.
- **WINS Server** – Enter the address of WINS Server to be used.
- **User Authentication** – Select the User Authentication method to be used.
- **Encryption Strength** – Select the Encryption Strength desired.
- **Use RADIUS Authentication:**
  Check the Use RADIUS Authentication button to enable RADIUS. Then the following information:
  - **RADIUS Port** – Select the port number.
  - **RADIUS Server IP Address** – Enter the RADIUS Server IP Address.
  - **Secret** – Enter a secret password.
  - **Secret Confirm** – Retype the secret password for verification.
- **Use Local Client List** – Check this radio button to have your local client list used by the program.

14. The **VPN Settings** screen for entering specific VPN settings will display. The **Connection Name** (**Site-A**) defaults into the first field. Select **Enable UID (Unique Identifier String)** and continue to enter the following settings:



a) Select **Enable UID**.

b) **Local IPSec Identifier –** Enter an IP address that identifies the Local IPSec for this connection. (Ex: **192.168.0.2**)

c) **Remote IPSec Identifier –** Enter an IP address that identifies the Remote IPSec for this connection. (Ex: **204.26.122.103**)

d) **Remote IP Network –** Enter the **Remote IP Network** address (**LAN**) for Site B. (Ex: **192.168.2.0**)

e) **Remote IP Netmask –** Enter the **Remote IP Netmask** address for Site B. (Ex: **255.255.255.0**)

f) **Remote Gateway IP –** Enter the **Remote Gateway IP** address (**WAN**) for Site B. (Ex: **204.26.122.103**). If Site B is using dynamic IP addressing, set this value to 0.0.0.0.

g) **Network Interface –** Select the **Network Interface** from the drop-down list box. (Ex: **WAN Ethernet**)

h) **Secure Association –** Select **IKE** to set how inbound packets will be filtered. **IKE** is the default. **IKE** primarily encompasses router key exchange and the negotiation of security policy. Selecting **IKE** displays field h-l.

i) **Perfect Forward Secure –** Check the **Enabled** button.

j) **Encryption Protocol** – Select the encryption protocol used for your configuration. The default protocol for the RF550VPN/RF560VPN communicating with another RF550VPN/RF560VPN is **3DES**. (Ex: **3DES**)

k) **PreShared Key –** Enter the **PreShared Key** name (you can enter an alphanumeric name but it needs to match the security code for the RouteFinder at Site B).

l) **Key Life –** Enter the amount of time that tells the router to renegotiate the Key. For example, 3600 seconds is 60 minutes.

m) **IKE Life Time –** Enter the amount of time that tells the router to renegotiate the IKE security association. For example, 28800 seconds is 8 hours.

15. Once the VPN settings are entered, click the **Save** button. The information will display on the VPN screen where you can enable/disable, edit or delete this connection by clicking the corresponding buttons. To enable this connection, check the **Enable** box that appears to the left of the connection name.

    Note: If you uncheck the **Enable** box, the parameters will remain on the screen for you to enable, edit, or delete.

16. After you have finished making all the changes on the various pages, click **Save and Restart** to save the settings and restart the device**.** After the restart, the device will function according to the saved settings.

17. During the save and restart process, system messages will let you know that you have successfully configured the settings for the device and saved the settings. You will see a status bar across the bottom of your browser showing the progress of the startup process. The RouteFinder home page will be loaded automatically after restart is completed.

This completes the configuration of the RF550VPN/RF560VPN at Site B.

Testing Your Configuration

You can test your connection between the two RouteFinders using the PING command at a DOS prompt. If a dynamic IP address is used to access the Internet at Site B, the PING will need to originate from Site B first before Site A can generate a successful PING directed at Site B.

1. At the Site B workstation connected to a LAN port of the RF550VPN/RF560VPN:
   a) At the DOS prompt PING the LAN port of the RF500S NAT Box at Site B.

      Example: PING 92.168.0.1 <return>

      You should see four successful packet transmit/receive statements. If you do not, try several more times. You may see several initial failures while the two devices make a connection.

   b) If this is successful, try to PING the WAN port of the RF500S NAT Box at Site B.

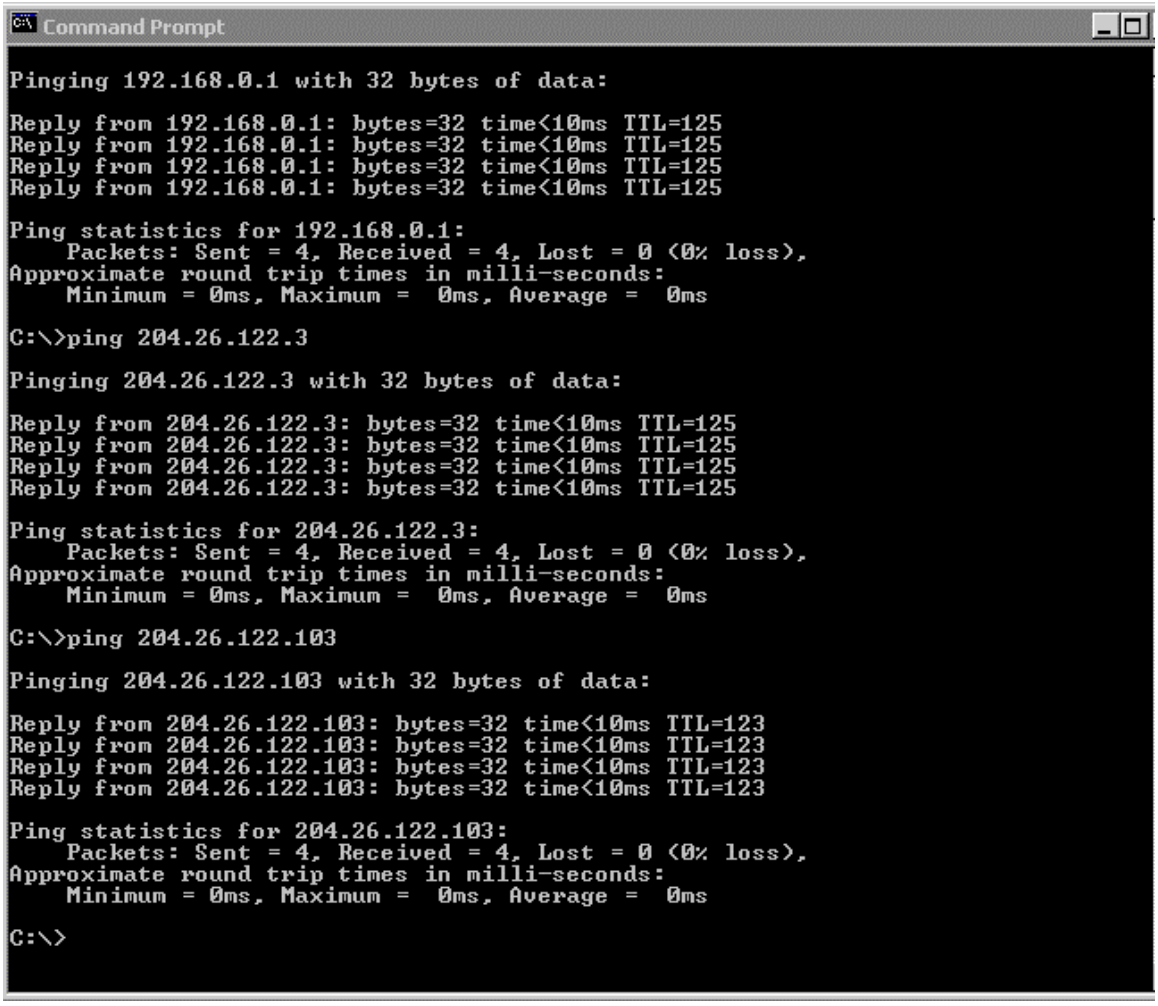
      Example: Ping 204.26.122.3

      You should see four successful packet transmit/receive statements. If you do not, try several more times. You may see several initial failures while the two devices make a connection.

   c) If this is successful, try to PING the WAN port of the RF550VPN/RF560VPN at Site A.

      Example: Ping 204.26.122.103

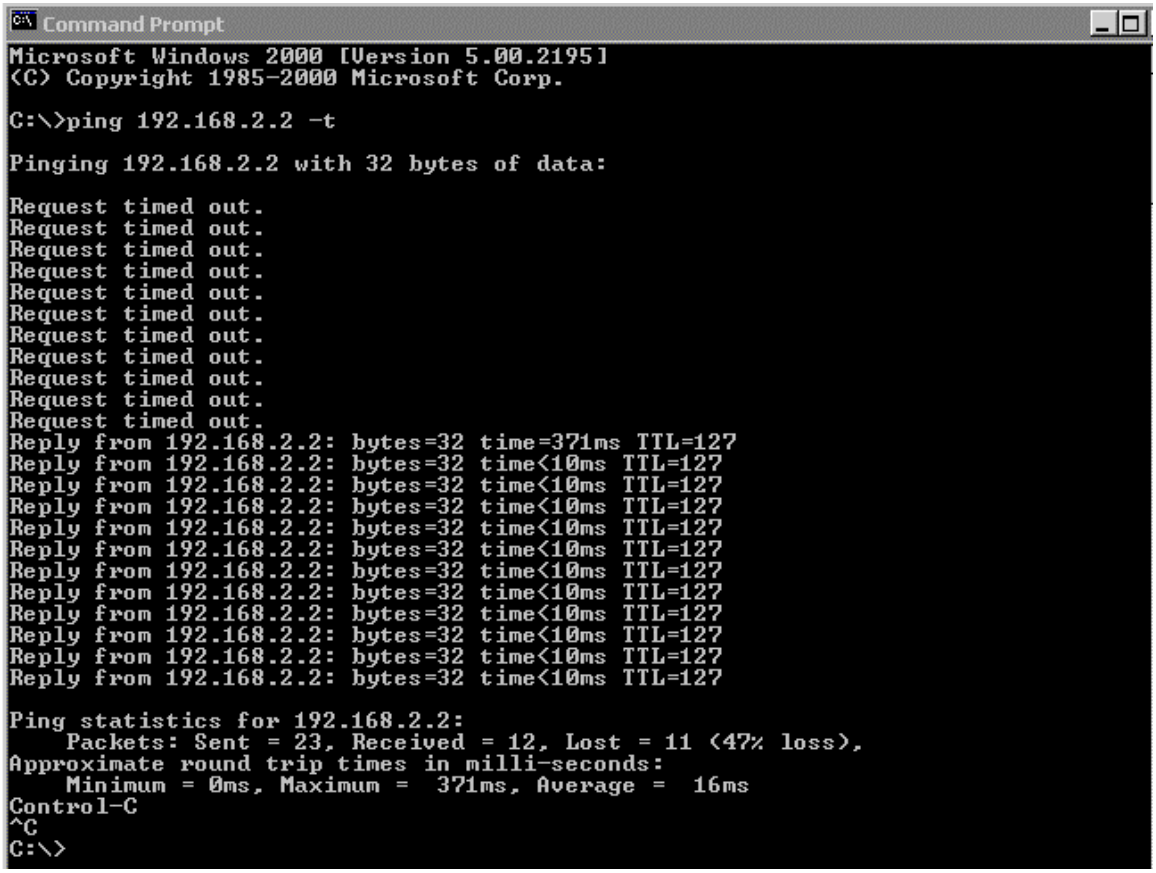
      You should see four successful packet transmit/receive statements. If you do not, try several more times. You may see several initial failures while the two RouteFinders make a secure connection



d) If this is successful, try to PING a workstation connected to the LAN port of the RF550VPN/RF560VPN at Site A.

Example: PING 92.168.2.2 <return>

You should see four successful packet transmit/receive statements. If you do not, try several more times. You may see several initial failures while the two RouteFinders make a secure connection.



Note: If any of these tests fail then verify that the workstations are connected to the LAN ports of the RF550VPN/RF560VPNs. The LAN port LINK LED should be on and the ACT LED should blink on each time you PING the RF550VPN/RF560VPN. Verify the WAN port at each Site is connected properly. Also verify that the RF550VPN/RF560VPNs and NAT Box are configured properly.